OPENCHAIN

Artificial Intelligence System Bill of Materials

Compliance Management Guide for the Supply Chain

An official guide published by the OpenChain Project (www.openchainproject.org)

Version 1.0

This page intentionally left blank

Table of Contents

Table of Contents 3

Introduction 5

1. Scope 7

2. Terms and Definitions 7

2.1 Artificial Intelligence (AI) 7

2.2 Artificial Intelligence System Bill of Materials (AI SBOM) 7

2.3 Artificial Intelligence System Bill of Materials Compliance (AI SBOM Compliance) 8

2.4 - compliance artifacts 8

2.5 - identified licenses 8

2.6 - program 8

2.7 - program participants 8

2.8 - supplied software 8

2.9 - verification materials 8

3. Guidance [3] 9

3.1 Policy 9

3.2 Competence 9

3.3 Awareness 10

3.4 Program scope 11

3.5 License obligations 11

3.6 Transparency obligations 12

3.7 Access 12

3.8 Effectively resourced 12

3.9 AI System Bill of Materials 13

3.10 Governance 13

Footnotes 15

This page intentionally left blank

Introduction

This guide defines the key requirements of a quality AI SBOM Compliance program. This objective is to provide a benchmark to build trust between organizations exchanging AI solutions. It is intended to help an organization consider how a program can be structured. It identifies key process points that can be included in such programs. This guide is under development and will likely see substantial changes and/or expansion before finalization.

This guide focuses on the "what" and "why" aspects of a program rather than the "how" and "when". This ensures flexibility for different organizations of different sizes in different markets to choose specific policy and process content that fits their size, goals and scope.

This guide was inspired by OpenChain ISO/IEC 5230 and considered how lessons learned from that specification could be applied to market requirements around AI SBOM management in the supply chain. Other ISO/IEC standards were also taken into account in the preparation of this guide. The primary references were:

ISO/IEC 5230:2020 https://www.iso.org/standard/81039.html [1]
ISO/IEC 42001:2023 https://www.iso.org/standard/81230.html
ISO/IEC 5962:2021 https://www.iso.org/standard/81870.html [2]

This page intentionally left blank

1. Scope

This document specifies the key requirements of managing AI compliance in the supply chain. It specifically focuses on using AI SBOM to accomplish this goal.

2. Terms and Definitions

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as:

"MUST" This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

"MUST NOT" This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

"SHOULD" This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

"SHOULD NOT" This phrase, or the phrase "NOT RECOMMENDED", mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

"MAY" This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

These definitions are originally from IETF RFC 2119: https://www.ietf.org/rfc/rfc2119.txt The OpenChain Project Specification Work Group reviewed the ISO definitions in 2023 to confirm no conflict: https://www.iso.org/foreword-supplementary-information.html

2.1 Artificial Intelligence (AI)

a computer system capable of performing tasks that would previously require human intelligence

2.2 Artificial Intelligence System Bill of Materials (AI SBOM)

a list of components and relevant information about the components that make up part or all of an AI system

2.3 Artificial Intelligence System Bill of Materials Compliance (AI SBOM Compliance)

a compliance activity related to AI that uses a bill of materials to support licensing, regulatory or business requirements

2.4 - compliance artifacts

a collection of artifacts that represent the output of a compliance program and accompany the supplied software

2.5 - identified licenses

a set of licenses identified as a result of following an appropriate method of identifying components from which the supplied software is comprised

2.6 - program

an organization's open source license compliance activities

2.7 - program participants

any organization employee or contractor that defines, contributes to or has responsibility for preparing, reviewing or approving supplied software

Note: Depending on the organization, that may include (but is not limited to) software developers, release engineers, quality engineers, product marketing, legal and product management.

2.8 - supplied software

software that an organization either provides or makes available to third parties

2.9 - verification materials

materials that demonstrate that a given requirement of the specification is satisfied

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

— ISO Online browsing platform: available at https://www.iso.org/obp

— IEC Electropedia: available at http://www.electropedia.org/

3. Guidance [3]

How an organization approaches and accomplishes compliance related to AI will depend on many factors. The size of the organization, the industry it operates in, the jurisdiction where it is based and the form of AI system, service, model, data or output will all be considerations in developing a program to support the compliance goal.

Without being too prescriptive, or going into too many details, we are trying to identify some of the key process points likely to be applicable to most organizations in most industries and most jurisdictions below. This is a living document and your input is actively solicited to help us refine the content.

Ideally the reader will review the process points or activities described below and be able to translate their existence and use into the development or refinement of their own compliance program related to AI.

3.1 Policy

A written policy shall exist that governs AI System Bill of Materials (AI SBOM) compliance. The policy shall be internally communicated, and informed by business strategy, legal requirements in the relevant jurisdictions, and the level of risk appropriate for the use case. [4]

Verification material(s):

- A documented policy meeting the above requirements
- A documented procedure that makes program participants aware of the existence of the policy (e.g. via training, internal wiki or other practical communication method)

Rationale:

To ensure steps are taken to create, record and make program participants aware of the existence of the policy. Although only high level requirements are provided in this section for what should additionally be included in the policy, other sections may impose specific obligations that must be included in the policy.

3.2 Competence

The organisation shall identify the roles and the corresponding responsibilities of those roles that affect the performance and effectiveness of the program; [5]

- Determine the necessary competence of program participants fulfilling each role. Program participants must have the requisite skills, knowledge, experience, and engagement with the functions below if relevant to the use case:
    - Governance
    - Security
    - Safety
    - Privacy

    - Development
    - Supplier management
- Ensure that program participants are competent on the basis of appropriate education, training, and/or experience;
- Where applicable, take actions to acquire the necessary competence; and
- Retain appropriate documented information as evidence of competence.

Verification material(s):

- A documented list of roles with corresponding responsibilities for the different participants in the program.
- A document that identifies the competencies for each role.
- Documented evidence of assessed competence for each program participant, with periodic checks to keep the list up-to-date.

Rationale:

To ensure the responsible people are accountable for their contributions.

3.3 Awareness

The organisation shall ensure that the program participants are aware of: [6]

- The AI SBOM policy;
- Relevant business objectives;
- Their contribution to the effectiveness of the program; and
- The implications of not following the Program's requirements.

Verification material(s):

- Documented evidence of assessed awareness for the program participants, which should include:
    - The program's objectives;
    - One's contribution within the program; and
    - The implications of program non-conformance.

Rationale:

- To ensure the program participants have obtained a sufficient level of awareness for their respective roles and responsibilities within the program.

3.4 Program scope

Different programs may be governed by different levels of scope. For example, a program could govern a single product line, an entire department, or an entire organisation. The scope designation needs to be declared for each program.

Verification material(s):

- A written statement that clearly defines the scope and limits of the program.

Rationale:

- To provide the flexibility to construct a program that best fits the scope of an organization's needs. Some organizations could choose to maintain a program for a specific product line while others could implement a program to govern the supplied software of the entire organization.

3.5 License obligations

A process shall exist for reviewing the relevant identified licenses for an AI system's code, weights, and datasets (including but not limited to training, testing, and verification datasets) as well as the license for the AI system itself to determine the obligations, restrictions, and rights granted by each license, taking into account the intended use of the AI system. Note that it's often the case that an AI system is trained on multiple other AI systems that may be identified in the AI system Model Tree for example; each of these may have their own licenses.

Verification material(s):

- A documented procedure to review and document upstream and downstream obligations, restrictions, and rights granted by each identified license, as appropriate.

Rationale:

- To ensure a process exists for reviewing and identifying the license obligations for each identified license for the various use cases an organization may encounter (as defined in ISO/IEC 5230:2020 Section 3.3.2).

3.6 Transparency obligations

A process shall exist for reviewing if there are any transparency obligations from regulations including but not limited to training, testing, and verification datasets, taking into account the intended use of the model.

If the use case for the training data creates a relevant issue (e.g., disclosure obligations to downstream recipients) in the context of transparency, then appropriate risk mitigation measures should be undertaken. [7]

Verification material(s):

- A documented procedure to review and document the transparency measures undertaken.

Rationale:

- To ensure that an organization is aware of the latest transparency obligations set out by regulators.

3.7 Access

Maintain a process to effectively respond to external AI SBOM Compliance inquiries. Publicly identify a means by which a third party can make an AI SBOM Compliance inquiry.

Verification material(s):

- Publicly visible method that allows any interested parties to make an AI SBOM Compliance inquiry (e.g., via a published contact email address). An internal documented procedure for responding to third-party AI SBOM Compliance inquiries. [8]

Rationale:

- To ensure there is a reasonable way for third parties to contact the organization with regard to compliance inquiries and that the organization is prepared to effectively respond.

3.8 Effectively resourced

- Identify and Resource Program Task(s):
    - Assign accountability to ensure the successful execution of program tasks.
- Program tasks are sufficiently resourced:
    - Time to perform the tasks have been allocated; and
    - Adequate funding has been allocated.
- A process exists for reviewing and updating the policy and supporting tasks;
- Legal expertise pertaining to AI SBOM Compliance is accessible to those who may need such guidance; and

- A process exists for the resolution of AI SBOM Compliance issues.

Verification material(s):

- Document with name of persons, group or function in program role(s) identified.
- The identified program roles have been properly staffed and adequate funding provided.
- Identification of expertise available to address AI SBOM Compliance matters which could be internal or external.
- A documented procedure that assigns internal responsibilities for AI SBOM Compliance.
- A documented procedure for handling the review and remediation of non-compliant cases.
- See, e.g., Sections B.4.2 and B.4.6 of Annex B of ISO/IEC 42001. Section B.9.3 from the same Annex also provides guidance to determine if human resources for human oversight should be incorporated.

Rationale:

- To ensure: i) program responsibilities are effectively supported and resourced and ii) policies and supporting processes are regularly updated to accommodate changes in AI SBOM Compliance best practices.

3.9 AI System Bill of Materials

A process shall exist for creating and managing an AI SBOM, this can be in any format e.g. SPDX, CycloneDX, or another format. The AI SBOM shall account for inbound materials from third-parties.

Verification material(s):

- A documented procedure for identifying, tracking, reviewing, approving, and archiving information related to the components of an AI system (e.g., model, datasets, etc).
- Records for the supplied system that demonstrates the documented procedure was properly followed.

Rationale:

- To ensure a process exists for creating and managing an AI SBOM used to construct the supplied system. A bill of materials is needed to support the systematic review and approval of the system to understand the obligations and restrictions

3.10 Governance

An organization shall have a governance framework for AI, policies, and practices to help ensure that AI systems are developed, deployed, and managed responsibly.

Governance emphasizes compliance with emerging AI laws and regulations, such as the EU AI Act, Hiroshima AI process or Global AI Governance Initiative (China), and addresses ethical considerations, risk management, and transparency. For example, understand the risks associated with ongoing use of AI Systems and training data in the context of their intended Programs. This could include the ability to monitor the lifecycle of the AI system and perform ongoing analysis of its intended uses. [9]

Verification material(s):

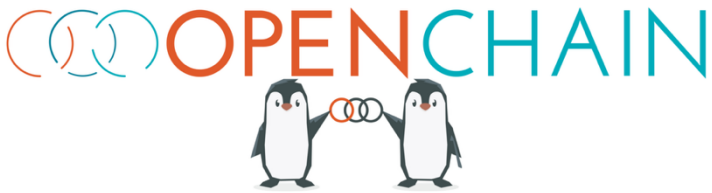
- A documented AI governance framework for the lifecycle of an AI system with a process to review the framework periodically.

Rationale:

- To ensure a process exists for maintaining an AI framework for the lifecycle of the AI system. A framework is needed to support the periodic review of the AI system.

Footnotes

1. OpenChain Project version: *OpenChain ISO/IEC 5230 - License Compliance* is functionally identical and freely available: https://openchainproject.org/license-compliance
2. SPDX Project version: *https://spdx.dev/wp-content/uploads/sites/31/2023/09/SPDX-specification-2-2.pdf* is functionally identical and freely available
3. In a specification, this section may be called "Requirements," but given that this is a guide an explicit term is used to ensure understanding that the items below are recommended, not prescriptive.
4. See, e.g., Section B.2.2., Annex B of ISO/IEC 42001.
5. See, e.g., Section B.3., Annex B of ISO/IEC 42001.
6. See, e.g., Section 7.3 of ISO/IEC 42001.
7. See, e.g., Sections B.5.3, B.6.2.3, B.6.2.7, and B.7 of Annex B of ISO/IEC 42001.
8. See, e.g., Section B.8.5 of Annex B of ISO/IEC 42001.
9. See, e.g., Section B.6.2 of Annex B of ISO/IEC 42001



This guide is one of many documents created, shared and maintained by the OpenChain Project to support a more trusted supply chain.

Our vision is a supply chain where open source is delivered with trusted and consistent process management information.

Our mission is to make that happen.

We Maintain Standards:

OpenChain ISO/IEC 5230
The international standard for open source license compliance programs

OpenChain ISO/IEC 18974
The industry standard for open source security assurance programs

And we maintain over 1,000 documents of supportive reference material, ranging from policy templates to self-certification checklists to training guides.

Learn more and get everything for free at www.openchainproject.org