This document has been replaced by this updated and reformatted document: https://docs.google.com/document/d/1XHztgMALwnu2D02bmWYyXeW3wE_Jw199/edit#heading=h.x3i92tls8mld

OpenChain AI Work Group

AI Compliance BOM Management Guide

Draft Document

Foreword

This section of the document is heavily inspired by taking the content of ISO/IEC 5230 and thinking "what matches market requirements around AI BOM management in the supply chain" and "what does not match market requirements around AI BOM management in the supply chain".

ISO Standards used in this discussion

- **ISO/IEC 5230:2020** - Information technology — OpenChain Specification
  - OpenChain Project Version, available at the link: *OpenChain ISO/IEC 5230 - License Compliance*
  - ISO/IEC Version, available at the link: *https://www.iso.org/standard/81039.html*
  - Both versions are functionally identical.
- **ISO/IEC 42001:2023** Information technology — Artificial intelligence — Management system.
  - ISO/IEC Version, available at the link: *https://www.iso.org/standard/81230.html*
- **ISO/IEC 5962:2021** - Information technology — SPDX® Specification V2.2.1

- SPDX Version, available at the link: *https://spdx.dev/wp-content/uploads/sites/31/2023/09/SPDX-specification-2-2.pdf*
- ISO/IEC Version, available at the link: *https://www.iso.org/standard/81870.html*
- Both versions are functionally identical.

Potential guidance around AI BOMs

1. **Policy**

A written policy shall exist that governs AI Bill of Materials (AI BOM) compliance of the supplied model/system. 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. See, e.g., Section B.2.2., Annex B of ISO/IEC 42001.

Verification materials

- A documented policy
- 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 no requirements are provided here on for what should be included in the policy, other sections may impose requirements on the policy.

2. **Competence**

The organisation shall identify the roles and the corresponding responsibilities of those roles that affects the performance and effectiveness of the program;

- Determine the necessary competence of program participants fulfilling each role
- 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.

3. **Awareness**

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

- The AI BOM policy;
- Relevant AI 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.

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.

5. **License obligations**

A process shall exist for reviewing the relevant identified licenses for a model's datasets (including but not limited to training, testing and verification datasets) as well as the model/system itself to determine the obligations, restrictions and rights granted by each license, taking into account the intended use of the model.

Verification material(s):

- A documented procedure to review and document the 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 §3.3.2).

6. **Transparency obligations**

A process shall exist for reviewing if there are any transparency obligations from regulations for a model's datasets (including but not limited to training, testing and verification datasets), taking into account the intended use of the model. *If a transparency obligation is required then it must be acted on.*

If training data is to be published and it contains data that contains personal identifiable data then this should be encrypted to allow others to use the general data sets without the personal data.

enthusiastic compliance

Verification material(s):

A documented procedure to review and document the transparency obligations

7. **Access**

Maintain a process to effectively respond to external AI compliance inquiries.

Publicly identify a means by which a third party can make an AI compliance inquiry.

Verification material(s):

Publicly visible method that allows any third party to make an AI compliance inquiry (e.g., via a published contact email address). An internal documented procedure for responding to third party AI compliance inquiries.

Rationale:

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

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 compliance is accessible to those who may need such guidance; and
- A process exists for the resolution of AI 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 compliance matters which could be internal or external.
- A documented procedure that assigns internal responsibilities for AI compliance.
- A documented procedure for handling the review and remediation of

non-compliant cases.

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 compliance best practices.

9. **AI content review and approval**

   There should be a process to review the AI content and have a compliance approvals process. There should also be a process for tracking new regulations and informing those in the project of any additional compliance requirements.

10. AI Bill of materials

A process shall exist for creating and managing an AI bill of materials, this can be in any format e.g. SPDX, CycloneDX or other format.

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 BOM 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

10. **Governance**

    An organization shall have a process framework to review and understand the

current regulations from AI models and training data perspective for their intended Programs. This could include the ability to monitor the lifecycle of the AI model and perform dynamic impact analysis. Organisations that have a Responsible AI (RAI) framework established should also have a process to manage the overall lifecycle of the AI models and datasets.