Automotive SBOM Action Plan

2025.11.11

Mission

Accelerate Smart and Effective SBOM Usage in Automotive Industry

For this purpose, we would like to...

Identify key challenges, concerns, and barriers to effective SBOM adoption in the automotive industry

So, we decided to...

Establish a collaborative community to share and discuss best practices for SBOMs in the automotive industry

Promote awareness and position Automotive SBOM as best practices across the automotive industry

Goal

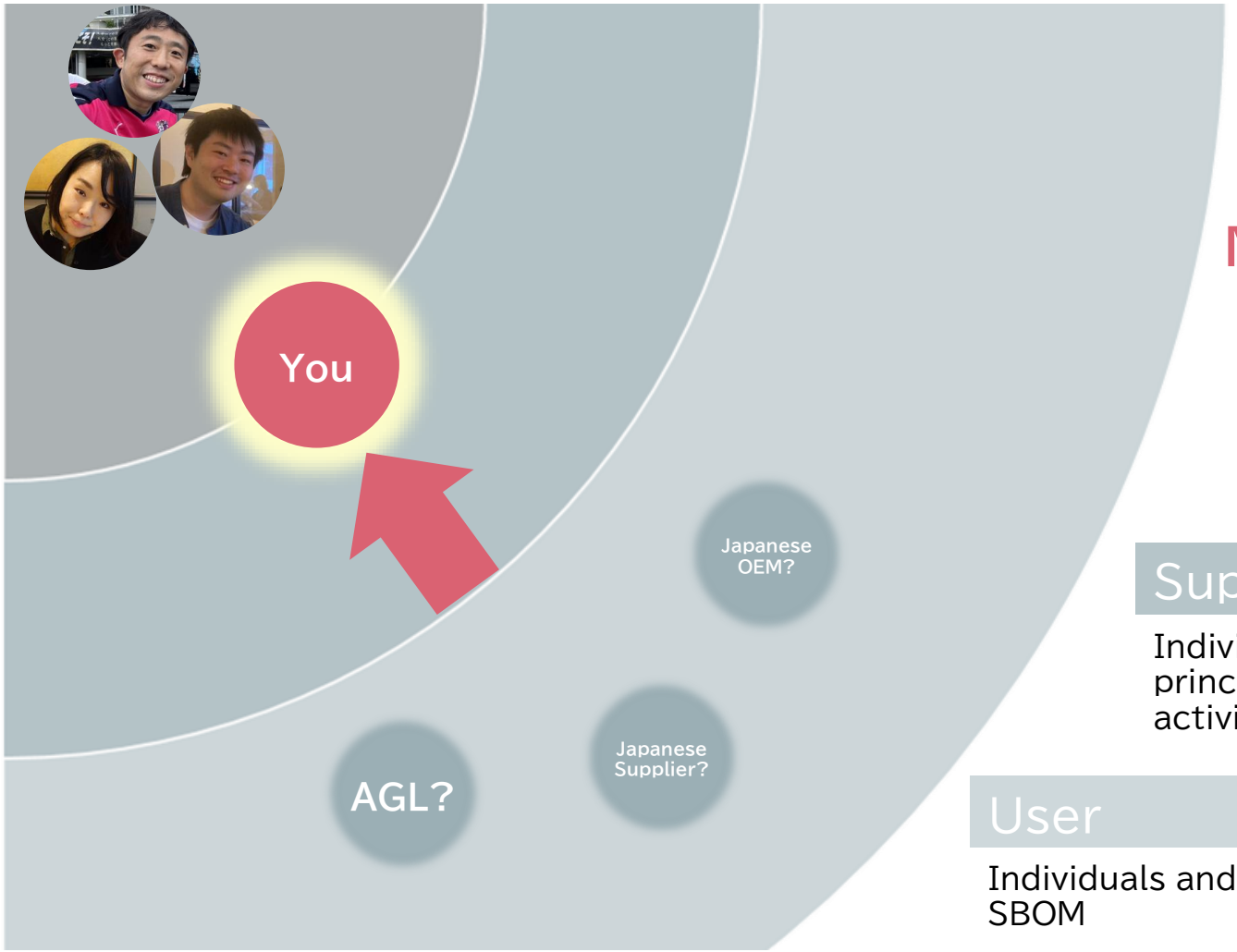
Future Goal

- Build a dynamic, collaborative community to drive the advancement of Automotive SBOMs
- Gain strong **endorsements from leading industry associations** to position Automotive SBOMs as best practices
- Establish Automotive SBOM as a **referenced standard within industry guidelines and legal requirements**

Near-Term Strategic Goal

- Increase industry awareness and drive **broader adoption** of Automotive SBOM **across the entire supply chain** (from OEMs to **Tier-N suppliers**)
- **Finalize** Automotive SBOM as the industry's best practice for smart and effective SBOM implementation, **incorporating feedback from community (you!!)**

Join us



Multiple Approaches to Support...

Contributor

Individuals and organizations actively engaged in the evaluation, advocacy, and utilization of Automotive SBOM

Supporter

Individuals and organizations that understand the principles of Automotive SBOM and support contributor activities

User

Individuals and organizations that adopt and leverage Automotive SBOM

Motivation and Key Interest of Contributors (Case1 : Toyota)

Key challenges in SBOM usage at Toyota

- Engineers and tools use SBOM formats (SPDX, CycloneDX) differently.
- Companies interpret items inconsistently.
- CS member struggle with mismatched data for vulnerability and license identification.
- Automotive industry: deep supply chain tiers, limited cross-company source sharing.

Toyota has started to consider SBOM Quality Standard

・Different standards from each OEM
→ Supplier burden
・No supplier input
→ Unrealistic SBOM practices, hard-to-document low-value items

- Automotive SBOM is a **collaborative effort** among related companies, not enforced by a single company.
- Aims to **eliminate ambiguity** and **resolve operational issues**.
- Builds on existing industry proposals, complies with regulations, and offers **clear strategies** and **action plans**.
- Enhances software reliability and transparency across all components — **OSS, proprietary, and COTS** — beyond traditional license compliance and vulnerability management.

Motivation and Key Interest of Contributors (Case2 : Hitachi Solutions)

As SBOM Consultant

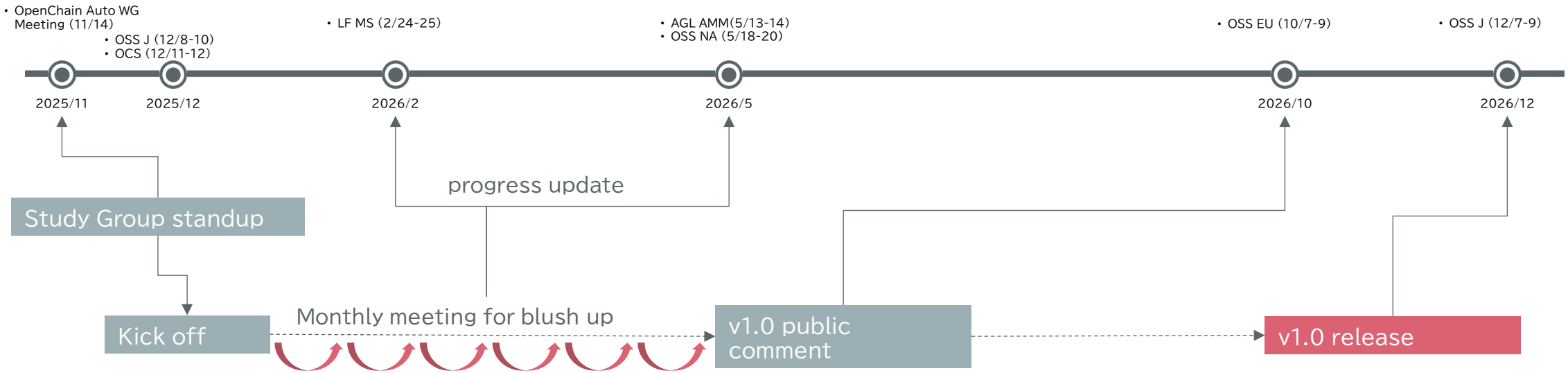
- Automotive industry customers face diverse challenges, concerns, and uncertainties
- These are common issues across the sector – let's collaborate to discuss and **solve them together**
- Share the outcomes and leverage them for effective implementation

As SCA Tool Distributor

- Few SCA tools satisfy automotive SBOM demands
- Speak with **ONE VOICE** to influence vendors and drive tool innovation

Roadmap

Events



Actions

Key Points

from the draft of Automotive SBOM

Background

Challenges of SBOM Implementation in the Automotive Industry

Multiple Standards Cause Confusion

Industry Specific Business Practices and Development Methods

Study is still in Progress

Automotive SBOM

We have reconsidered the content to focus on operations in the automotive industry, and defined an Automotive SBOM as an SBOM specification that follows the general-purpose SBOM specification.

Purpose of Automotive SBOM

1 Use as a Common Standard in the Supply Chain

- Automotive SBOM defines the format, data content, and granularity of the information that OEMs requires.
- Being used in suppliers as a common guideline for creating SBOMs that meet quality criteria, Automotive SBOM improve transparency and traceability throughout our supply chain.

2 Contribution to Improving Productivity in the Automotive Industry

- Automotive SBOM was designed with the intention to be commonly used by OEMs both in Japan and overseas.
- By standardizing the requirements from OEMs to suppliers, the burden on suppliers to comply with multiple requests from OEMs will be reduced.

3 Use as a Requirement Specification for Tool Vendors

- The content of SBOM can be collected by using SCA tool, but the functions and performance of the SCA tools currently available on the market are not perfect.
- Automotive SBOM can be used as a means of concretely communicating feature enhancement requirements to SCA tool vendors, and as a criterion for tool selection by each development team.

Configuration of Automotive SBOM

Data Fields	Definition of Data Items to be Handled as SBOM
Automation Support	Definition of Document Format, Format of Each Data, and Implementation Examples
Practice and Process	Definition of Operational Procedures for Requesting, Generating, and Using SBOM

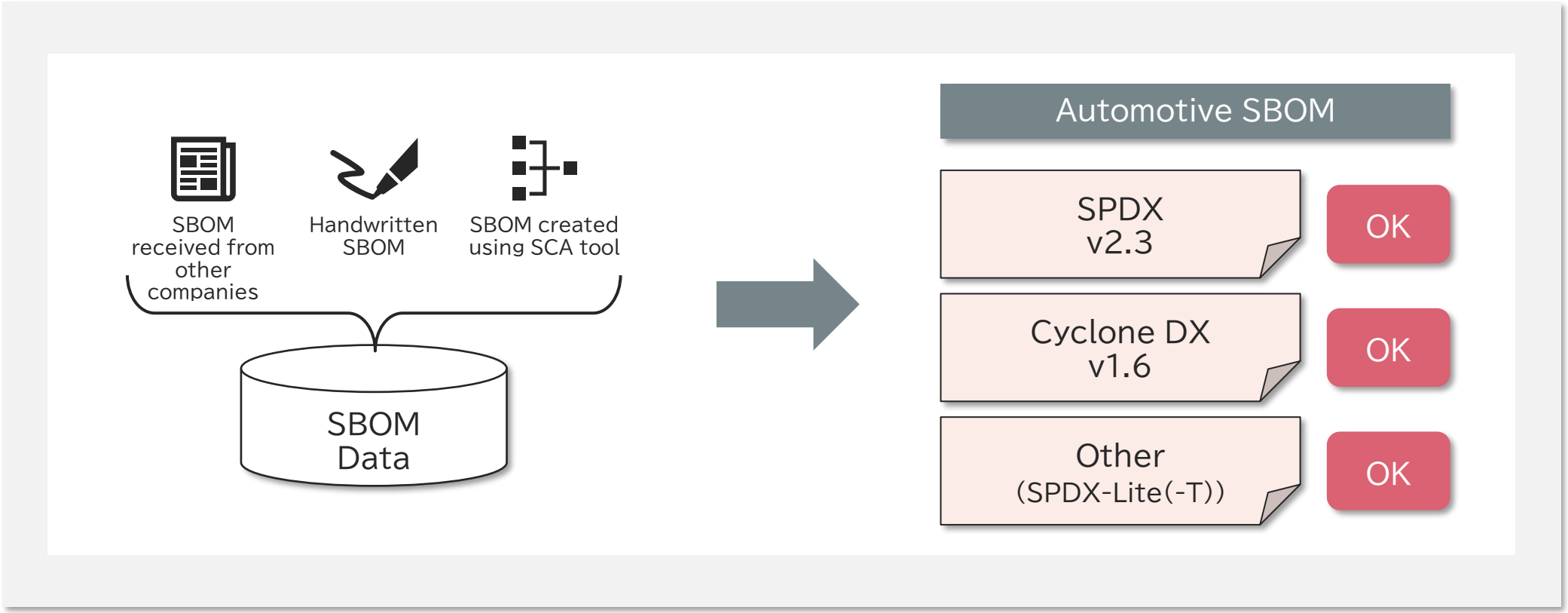
Data Fields

Defined as the Minimum Data Set Required to Understand the Configuration Information of the Target Software

#	Name of Data Field	Required	Description	Example
1	SBOM Metadata			
1-1	SBOM Author Name	○	Name of the entity that created the SBOM	“TOYOTA MOTOR CORPORATION”
1-2	SBOM Timestamp	○	Date and time when the SBOM was created or updated	“2025-01-24T22:31:37Z”
1-3	SBOM Type	○	Information to identify when and what types of software the SBOM was generated from	(Using SBOM type like “Build” etc.. which is defined by CISA at USA)
1-4	SBOM Primary Component	○	Information to identify the components that are primarily represented in the SBOM	(Express by using Component entities#2)
2	Component Attribute			
2-1	Component Name	○	Name of the component	“Apache Tomcat”
2-2	Component Version	○	Version information of the component	“10.0.5”
2-3	Component Supplier Name	○	Name of the entity that provided the component	Woven by Toyota, Inc.
2-4	Component Relationship	○	Information to identify dependencies between components	(Express following document format)
2-5	Component Unique Identifier	○	Information to uniquely identify the component	”pkg:github/apache/tomcat”
2-6	Component File Name	-	Name of the file of the component	”tomcat-10.0.5.tar.gz”
2-7	Component Download Location	-	URL from which the component is downloaded	“https://github.com/apache/tomcat/...../10.0.5.tar.gz”
2-8	Component Declared License	-	License declared by the component’s author	Apache-2.0”
2-9	Component Concluded License	○	License that the SBOM author concluded applies to the component	“Apache-2.0”
2-10	Component Cryptographic Hash	-	Hash value of the component	”SHA256: 525……5a8”
2-11	Component Copyright Notice	○※	Copyright notice attached to the component	“Copyright © 1999-2022, The Apache Software Foundation”
2-12	Component External Document References	○	Information for external references to other SBOM documents	(Express following document format)

Recommended Data Format

Automation Support



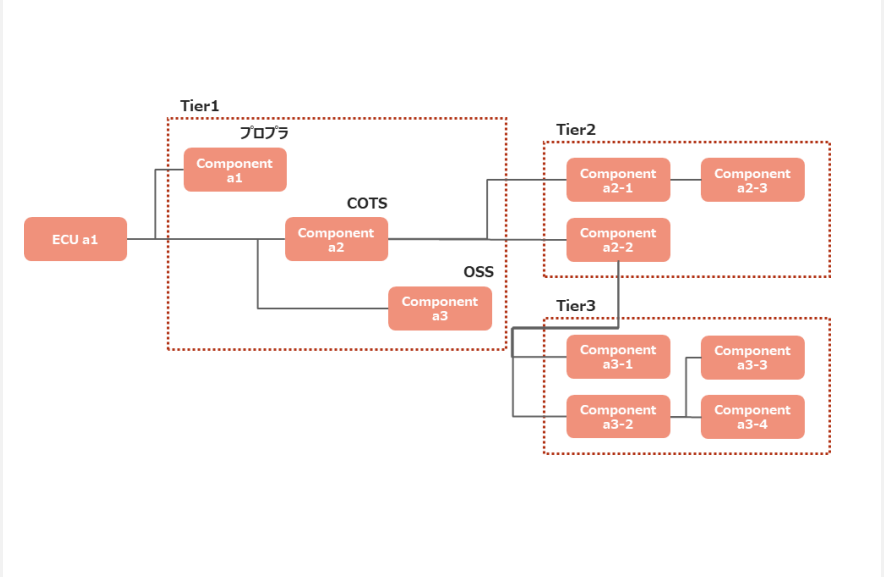
Any format is acceptable as long as it adheres to the Automotive SBOM data fields and practices and processes

Practice and Process

In a Single SBOM File

Disadvantages
- SBOM file becomes too large
- Time-consuming to recreate the entire SBOM file every time you update your software

Binding SBOMs Using External Reference Expressions



Advantages
- Easy to handle as a collection of small SBOMs
- High maintainability as there is no need to recreate the entire system every time a software update is made