Bildlizenz: imaginima/E+ via Getty Images

SBOM Management at Mercedes-Benz

Dr. Christian Wege, Aoileann Nic Chraith of Mercedes-Benz Group AG

Open Chain and Friends 2025
Stuttgart, 07.04.2025

Mercedes-Benz

In a nutshell…

With the **FOSS Disclosure Portal** we aim at a more efficient, digital, and transparent software supply chain regarding open source

Mission

Free & Open Source Software (FOSS) brings innovation, efficiency and speed,
but we need to make sure to play it save

FOSS Disclosure Portal

Software Bill of Materials (SBOM) provided by suppliers to our central inventory enables checking license conformance easier & faster

SBOM Management at Scale

FOSS SBOM consumption will intensify the collaboration with software suppliers and poses both opportunities and challenges

Software Bill Of Materials (SBOM) everywhere!

MAY 12, 2021

Executive Order on Improving the Nation's Cybersecurity

BRIEFING ROOM › PRESIDENTIAL ACTIONS

(vi) maintaining accurate and up-to-date data, provenance (i.e., origin) of software code or components, and controls on internal and third-party software components, tools, and services present in software development processes, and …

An official website of the United States government

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Cybersecurity > Software Bill of Materials

SOFTWARE BILL OF …

National Telecommunications and Information Administration
United States Department of Commerce

SOFTWARE BILL OF MATERIALS

A "Software Bill of Materials" (SBOM) is a nested inventory for software …

Bundesamt für Sicherheit in der Informationstechnik

Deutschland Digital•Sicher•BSI•

Die Lage der IT-Sicherheit in Deutschland 2021

Microsoft open sources its software bill of materials (SBOM) generation tool

Danesh Kumar Badlani, Adrian Diglio

July 12th, 2022

Linux Foundation Announces Software Bill of Materials (SBOM) Industry Standard, Research, Training, and Tools to Improve Cybersecurity Practices

THE LINUX FOUNDATION | 17 JUNE 2021

The Linux Foundation responds to increasing demand for SBOMs that can improve supply chain security

iX 10 – Was lauert in Ihrer Software? Angriffe auf die Software Supply Chain abwehren. Wie SBOMs Code-Abhängigkeiten sichtbar machen

c't magazin für computer technik 12 – Fatale Abhängigkeiten von fremdem Code meistern. Weckruf Log4j: Wenn Bibliotheken zur Katastrophe führen. Tools, mit denen Sie Problem-Code finden und vermeiden

INNOVATION

Know Your Part: Why Open Source Should Push For Software Bills Of Materials

Kevin Korte, Forbes Councils Member

Oct 7, 2022

Gartner Research

Innovation Insi…

Published: 14 February 2022

EU Cyber Resilience Act

For safer & more secure digital products

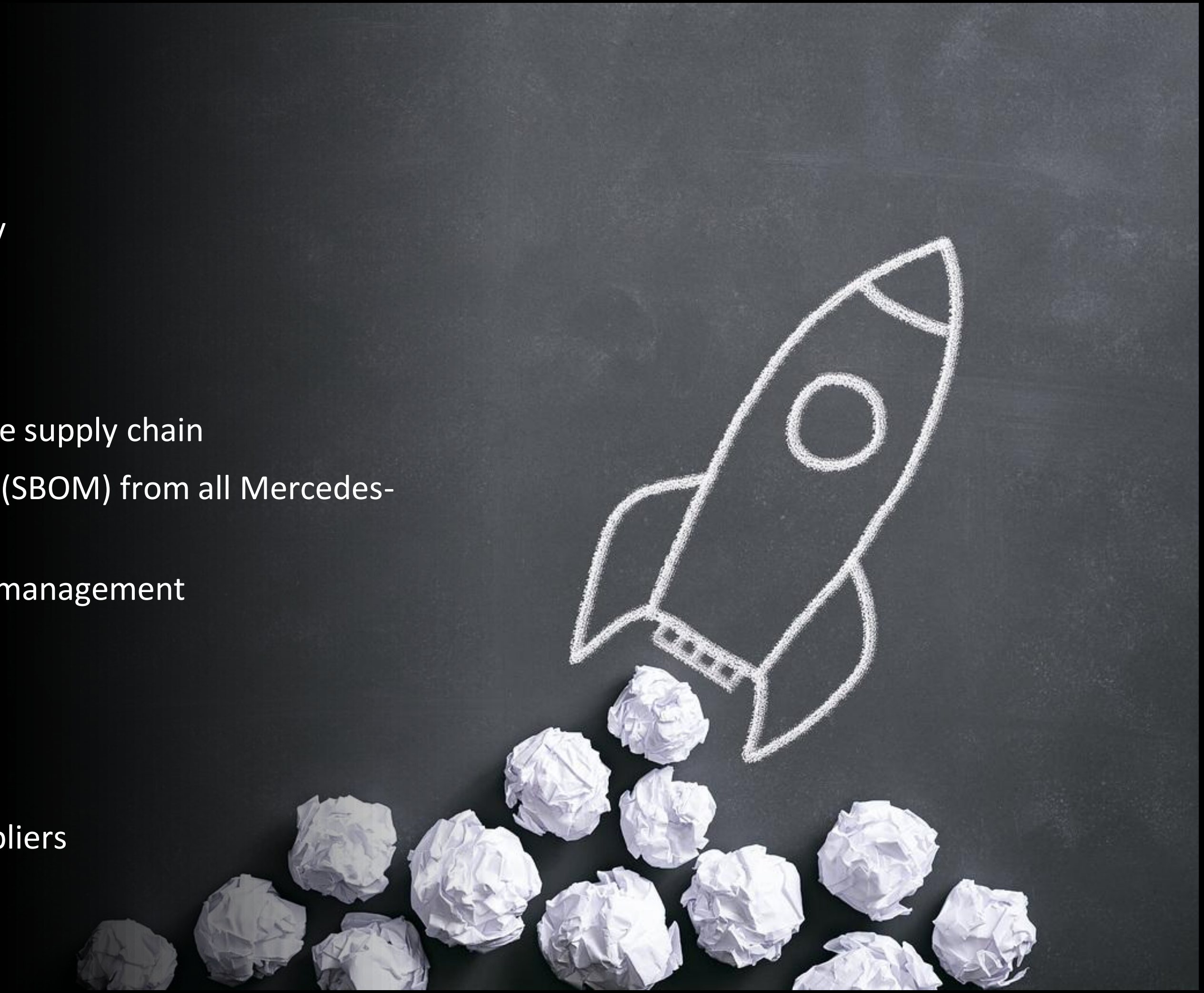
OpenChain Telco SBOM Guide: A Guide From The OpenChain Project

Version 1.0

What is a Software Bill Of Materials?

- The set of parts (packages) your software product depends on
- A package may add up further (transitive) dependencies
- A FOSS SBOM contains all meta data (name, version, license, copyright) for the FOSS packages used in a product

FOSS Disclosure Portal



Bildlizenz: ThomasVogel/iStockphoto via Getty Images

OUR VISION: WHAT IS IT?

- A more efficient, transparent and digital software supply chain
- Digitized and automated FOSS Disclosure Process
- Increased transparency leads to better license compliance and security

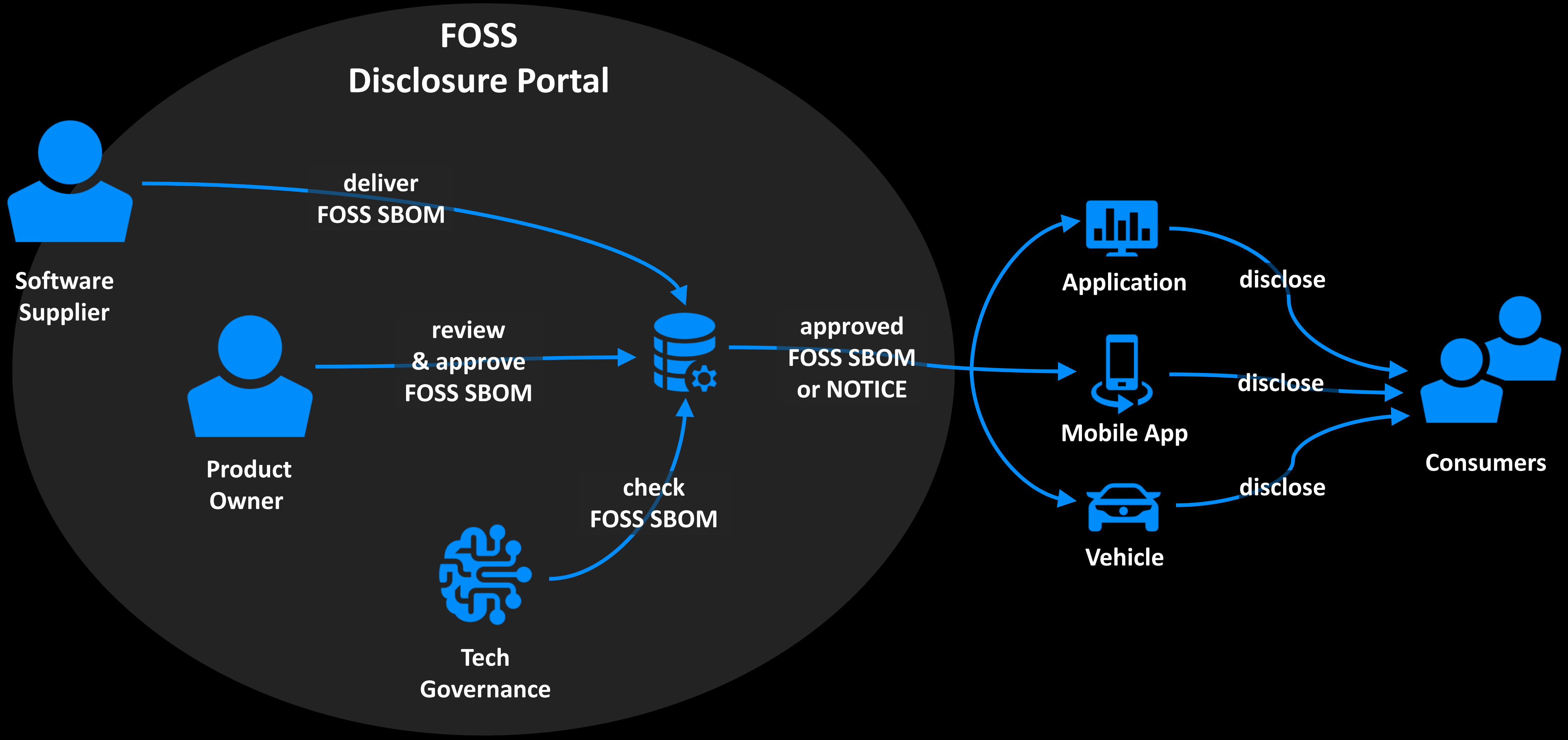
OUR MISSION: HOW DO WE ACHIEVE IT?

- With the FOSS Disclosure Portal we automate the open source software supply chain
- Create a central worldwide inventory of FOSS Software Bill of Material (SBOM) from all Mercedes-Benz companies with legal information for license checks
- Provide automation for guided conformance checking and obligations management

OUR PURPOSE: WHY DO WE STRIVE FOR IT?

- Be compliant, secure, and developer-friendly
- Make life easier for developers, application owners, and software suppliers
- Follow the company’s software compliance guidelines

FOSS SBOM in the Software Supply Chain



Open Source Options

Use one of these ...

- OSS Review Toolkit
- FOSS Light
- Hermine
- dependency track
- SW360
- DejaCode

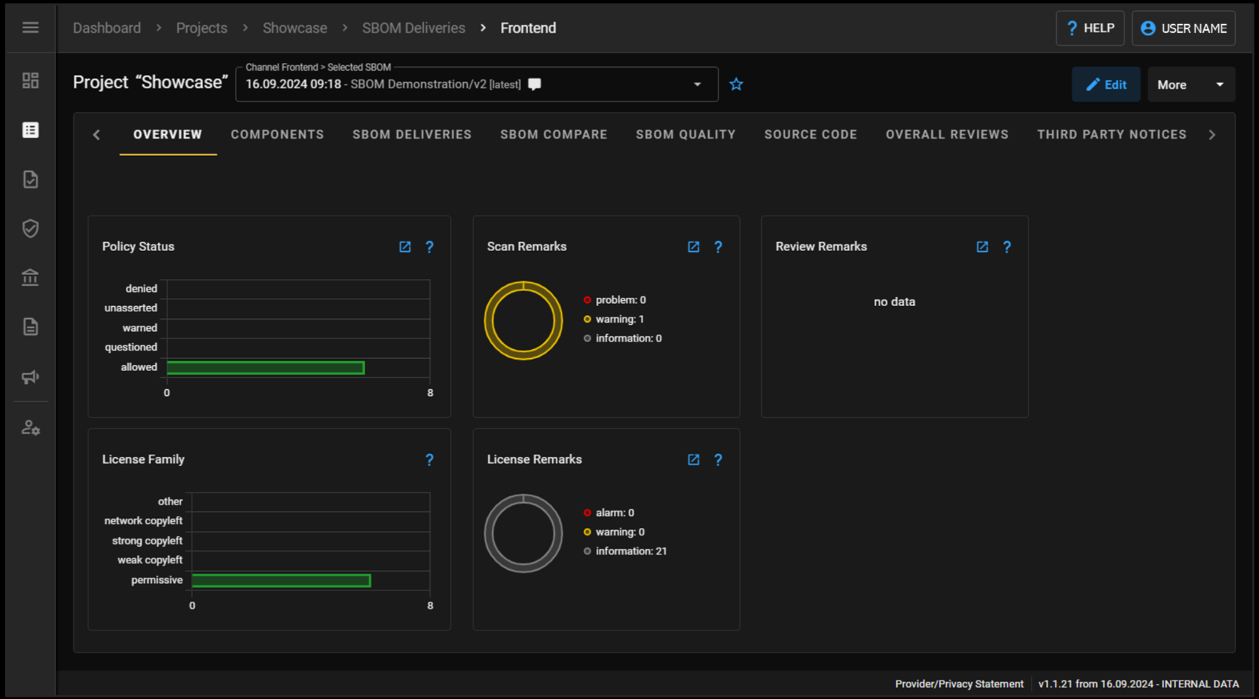
... or build your own

Bildlizenz: Christian Horz/iStockphoto via Getty Images

Benefits for Product Owners

ISO Format for SBOM Exchange

REST API & CLI for CI/CD Integration



Project “Showcase”

Channel Frontend > Selected SBOM: 16.09.2024 09:18 - SBOM Demonstration/v2 [latest]

Policy Status

Scan Remarks

- problem: 0
- warning: 1
- information: 0

Review Remarks

no data

License Family

License Remarks

- alarm: 0
- warning: 0
- information: 21

Provider/Privacy Statement | v1.1.21 from 16.09.2024 - INTERNAL DATA

UI/UX Design for Ease of Use

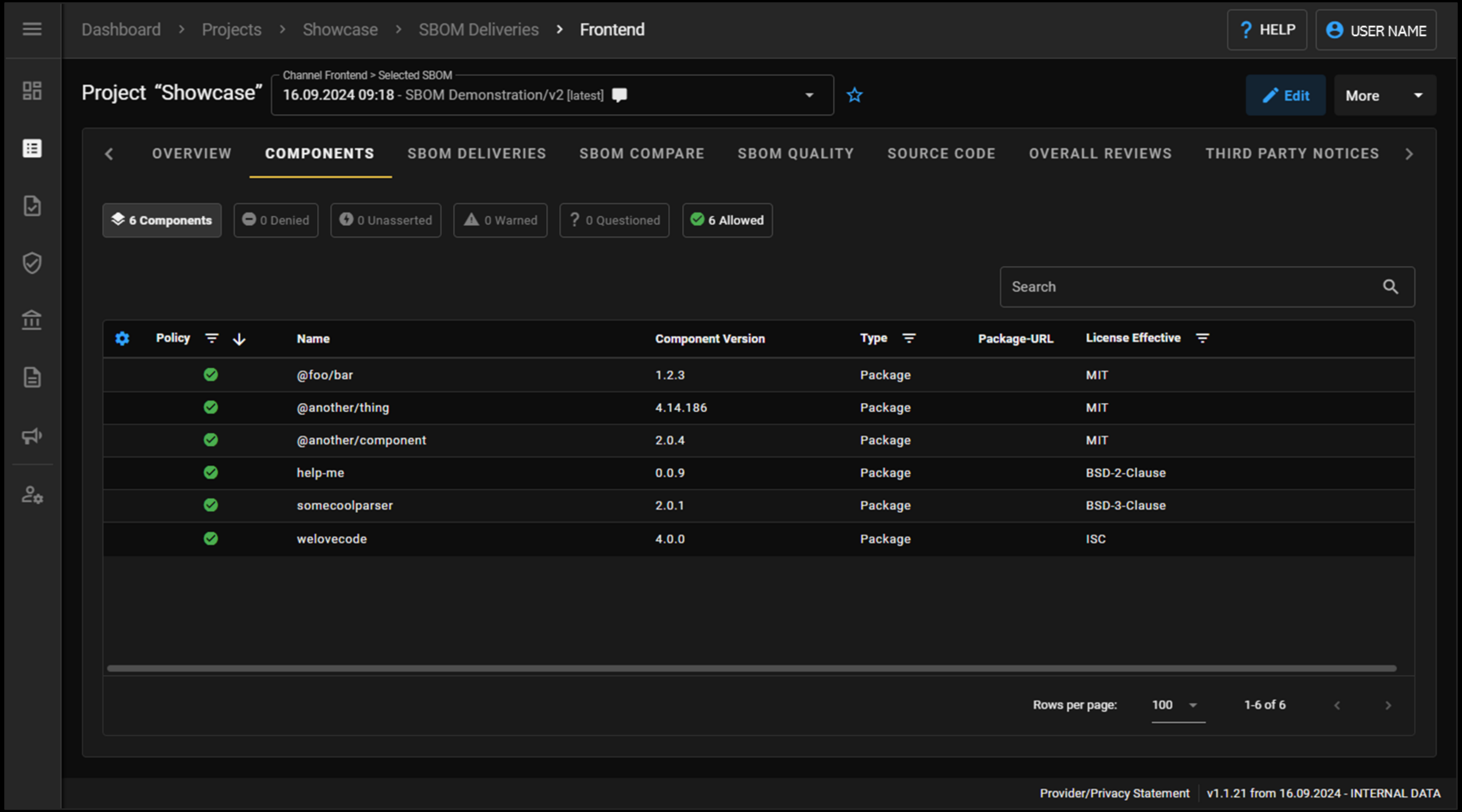
Notice Generation for Disclosure

License Database for Legal Guidance

Policy Rules for Compliance

Quality Checks for Obligations Management

Example: Components of an SBOM



Project “Showcase”

Channel Frontend > Selected SBOM
16.09.2024 09:18 - SBOM Demonstration/v2 [latest]

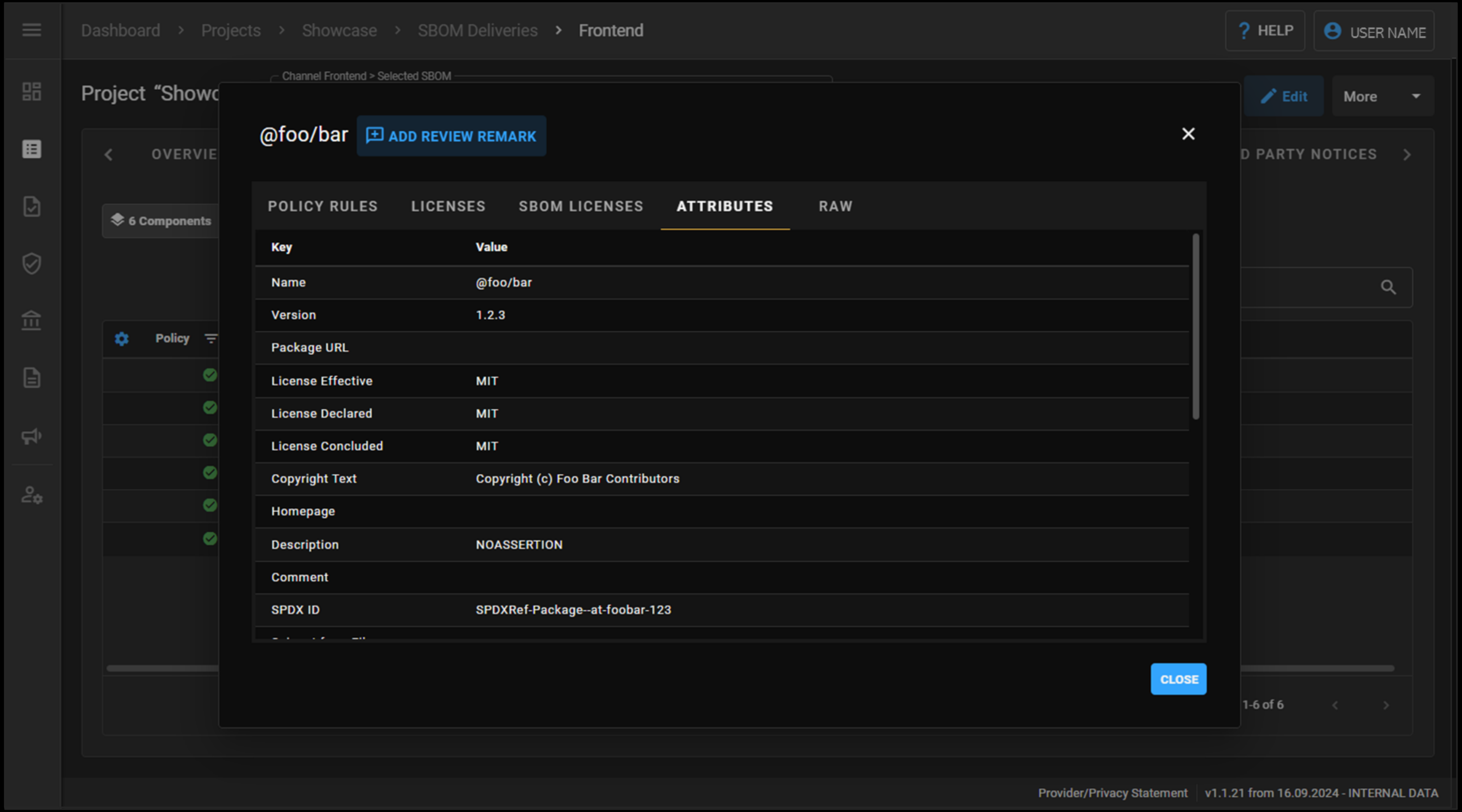
6 Components | 0 Denied | 0 Unasserted | 0 Warned | 0 Questioned | 6 Allowed

Policy	Name	Component Version	Type	Package-URL	License Effective
✓	@foo/bar	1.2.3	Package		MIT
✓	@another/thing	4.14.186	Package		MIT
✓	@another/component	2.0.4	Package		MIT
✓	help-me	0.0.9	Package		BSD-2-Clause
✓	somecoolparser	2.0.1	Package		BSD-3-Clause
✓	welovecode	4.0.0	Package		ISC

Rows per page: 100 1-6 of 6

Provider/Privacy Statement | v1.1.21 from 16.09.2024 - INTERNAL DATA

Example: Details of a Component

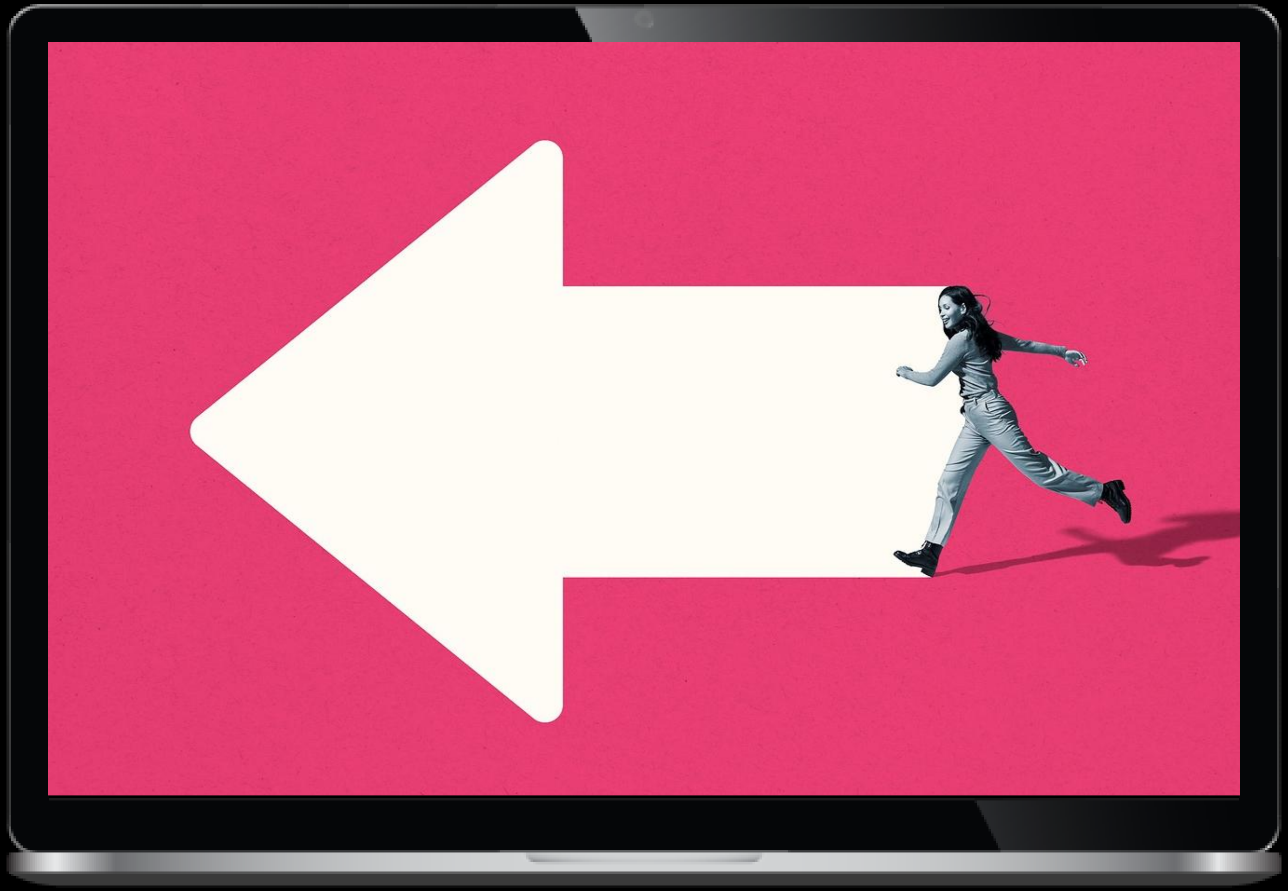

Dashboard > Projects > Showcase > SBOM Deliveries > Frontend
? HELP
USER NAME
Channel Frontend > Selected SBOM
Project "Showc
Edit
More
OVERVIE
D PARTY NOTICES
6 Components
Policy
1-6 of 6
ADD REVIEW REMARK
POLICY RULES
LICENSES
SBOM LICENSES
ATTRIBUTES
RAW
CLOSE
Provider/Privacy Statement
v1.1.21 from 16.09.2024 - INTERNAL DATA

@foo/bar

Key	Value
Name	@foo/bar
Version	1.2.3
Package URL	
License Effective	MIT
License Declared	MIT
License Concluded	MIT
Copyright Text	Copyright (c) Foo Bar Contributors
Homepage	
Description	NOASSERTION
Comment	
SPDX ID	SPDXRef-Package--at-foobar-123

SBOM Challenges

- Common Identifiers
- Data Quality and Curating
- Required Attributes
- Obligations and Abstraction
- All Code of All Dependencies
- Worldwide rollout



Bildlizenz: iStock.com/DigitalVision/Klaus Vedfelt