SOAFEE

SDV時代のオープンソースとソフトウェアサプライチェーンマネジメントの推進

Promoting Open Source and Software Supply Chain Management in the SDV Era

Masato ENDO (Open Chain Project Automotive Chair)

15th May,2025

Masato ENDO

-Project General Manager,
-Manager of OSPO
TOYOTA Motor Corporation

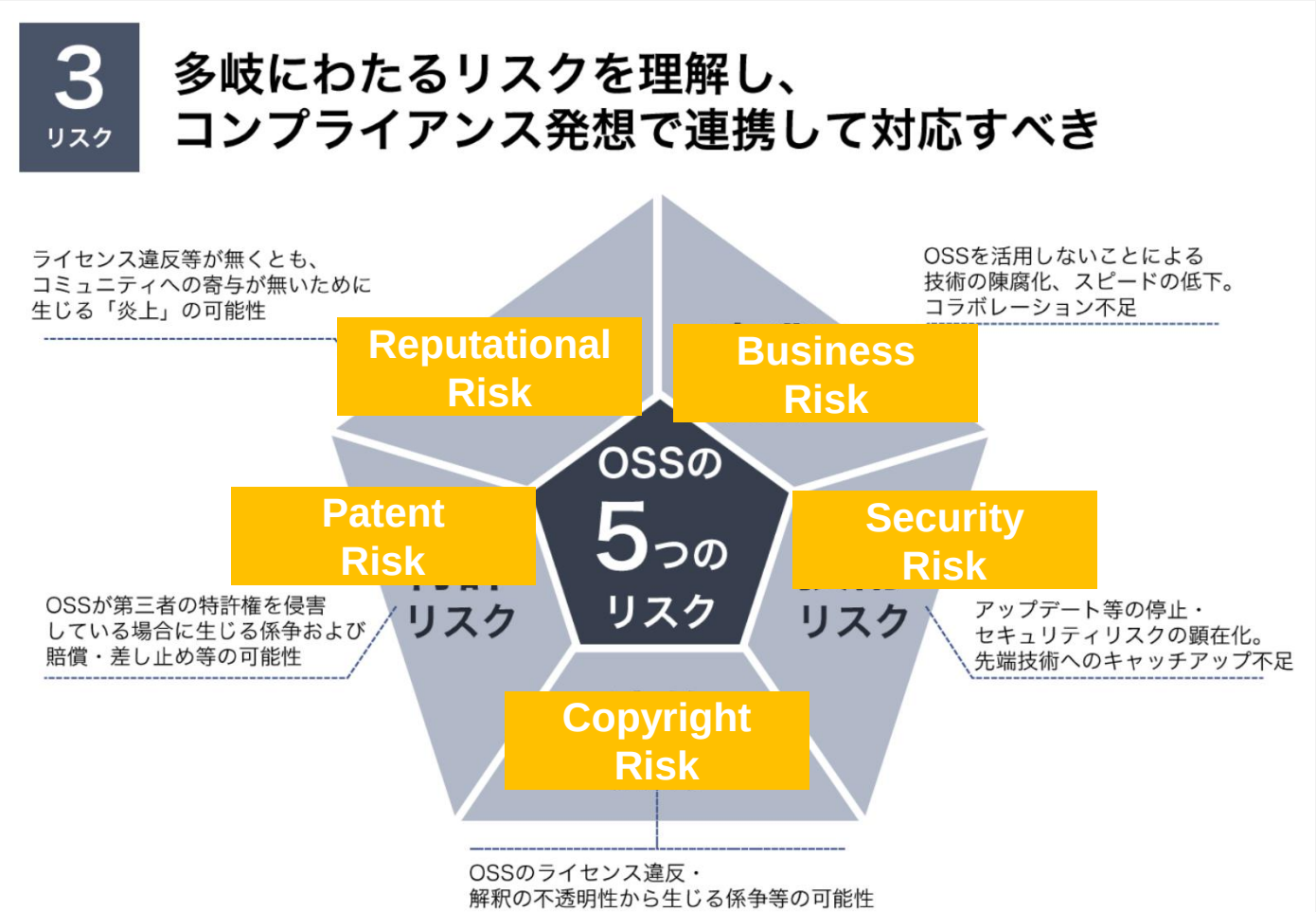
Automotive Chair,
The Linux Foundation
OpenChain Project

THE LINUX FOUNDATION
JAPAN EVANGELIST

JAPAN EVANGELIST
The Linux Foundation

Fellow,
United States Japan
Leadership Program

5 Risks of OSS



特許庁・内閣府　知的財産推進事務局　Opensource for ALL
https://www.jpo.go.jp/resources/report/takoku/document/zaisanken_kouhyou/2019_06_2.pdf

OSS License

- The OSS source code contains a license which indicates how the OSS author intends the source code to be used.
- Violating the license may be considered a breach of contract or copyright violation. In the worst case, it may become necessary to stop providing the products or service.

GPL

When a GPL OSS (including modified OSS) is released, it is necessary to also disclose the source code, including from other software which the OSS links to (copyleft).

BSD

Requirements for redistribution include a statement indicating the lack of a guarantee, and presentation of the copyright and license terms. There is no obligation to disclose the source code.

MIT

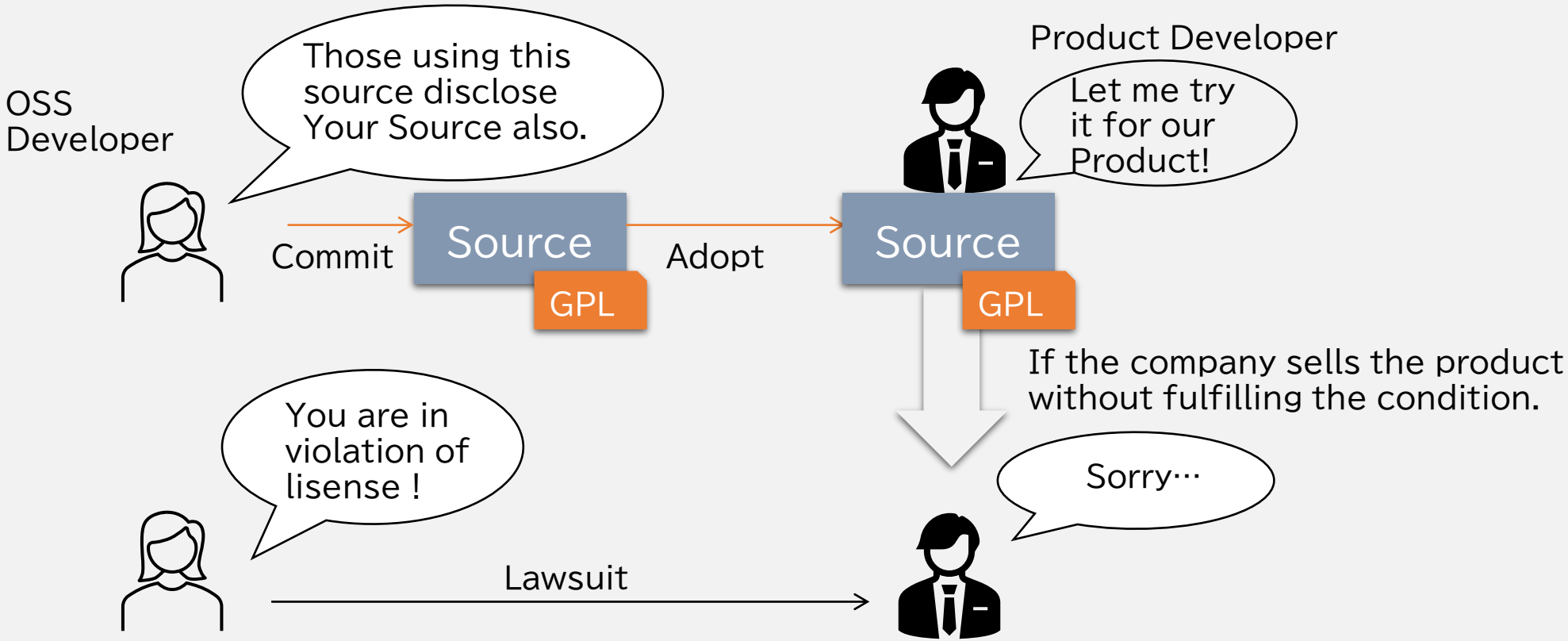
Required to indicate the copyright and the license text in the software.
Can be used for free and without restriction.
There is no guarantee.
There is no obligation to disclose the source.

Apache2.0

BSD-based.Patent rights granted free of charge.

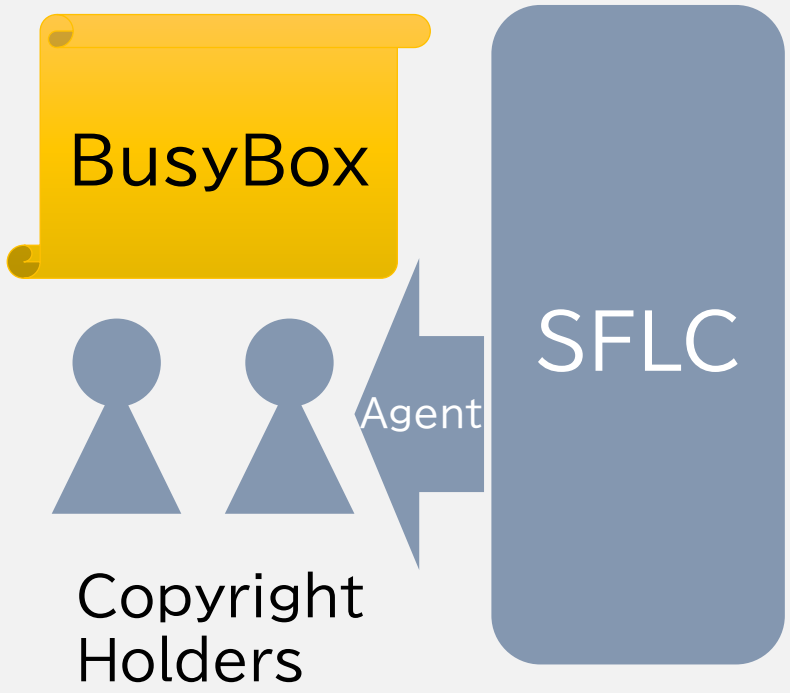
Copyright management of OSS

- Each OSS package comes with its own license, violation of which is a copyright violation and the product using the source code may be suspended from sale.
- The license may stipulate obligations of publication of the modified source codes, security disclosure or non-assertion of patents.



BusyBox Case

- In 2009, Software Freedom Law Center (SFLC) sues 14 users of the OSS utility software "BusyBox" for violation of GPLv2



Sue

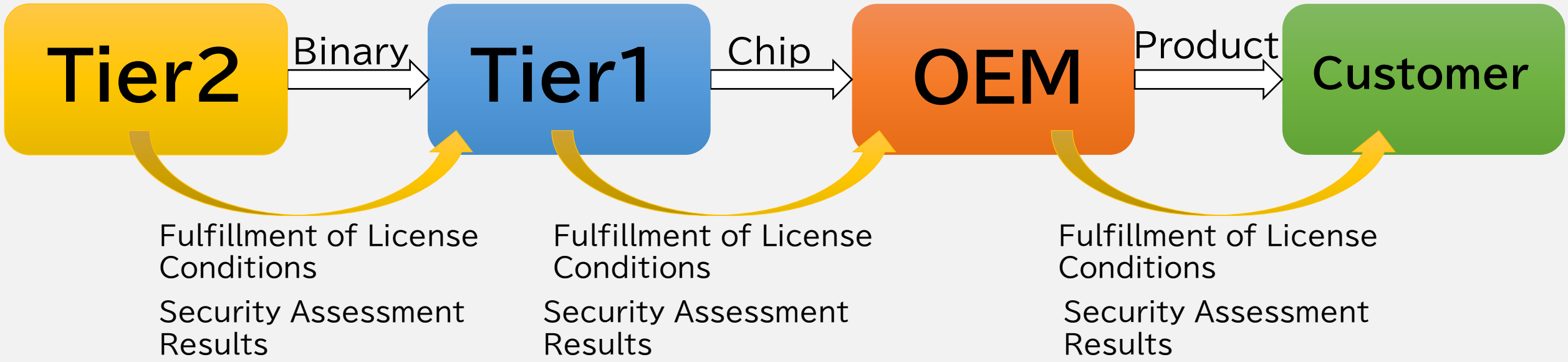
Astak
Best Buy
Comtrend
Dobbs-Stanford
GCI Technologies
Humax USA
JVC Americas Corporation
Phoebe Micro
Robert Bosch
Samsung Electronics
Versa Technology
Western Digital
Westinghouse
Zyxel Communications

Examples of Settlement Details
-Fulfillment of Obligations(Code disclosure)
-Payment of Settlement
-Appointment of an OSS Manager

Post Litigation Impact
Companies around the world are increasingly establishing Open Source Program Offices (OSPOs).

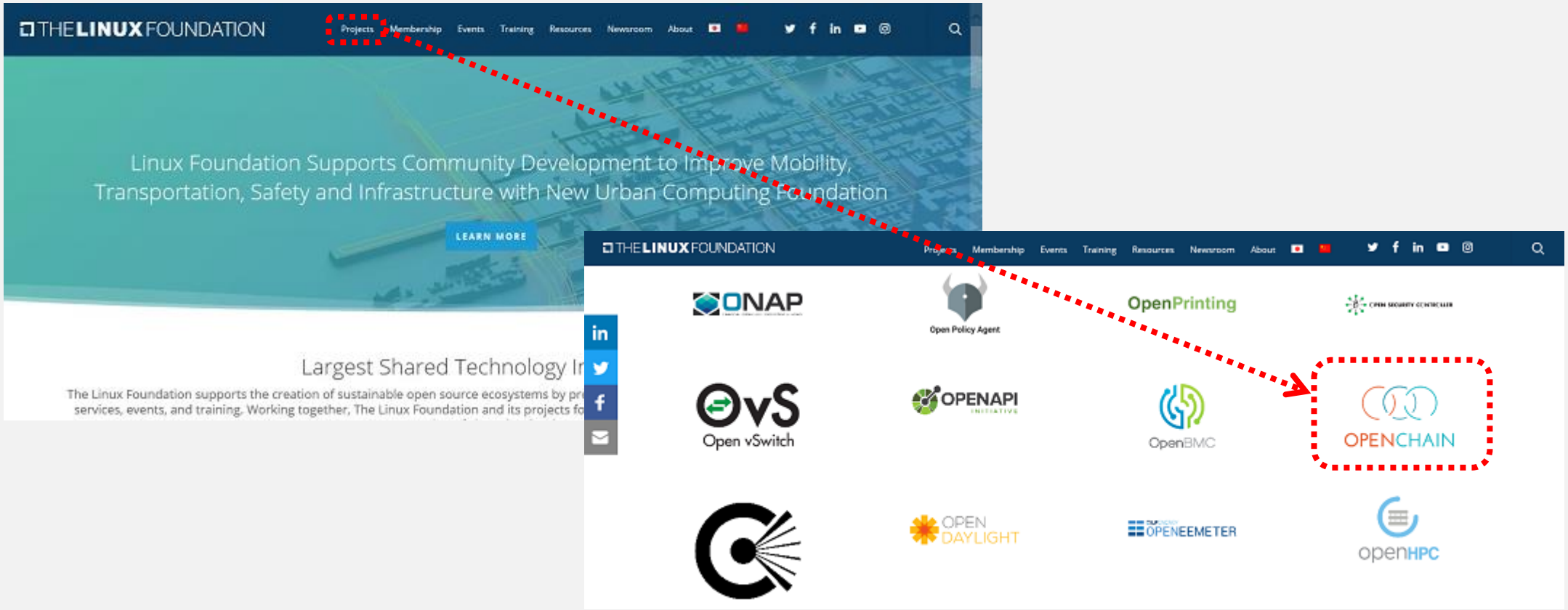
Supply Chain Risk of Open Chain

- You must fulfill your licensing obligations and inform security information to your customers.
- However, if the software is delivered as a chip or binary, it may be difficult to know what is in the software and what obligations are owed to the customer.



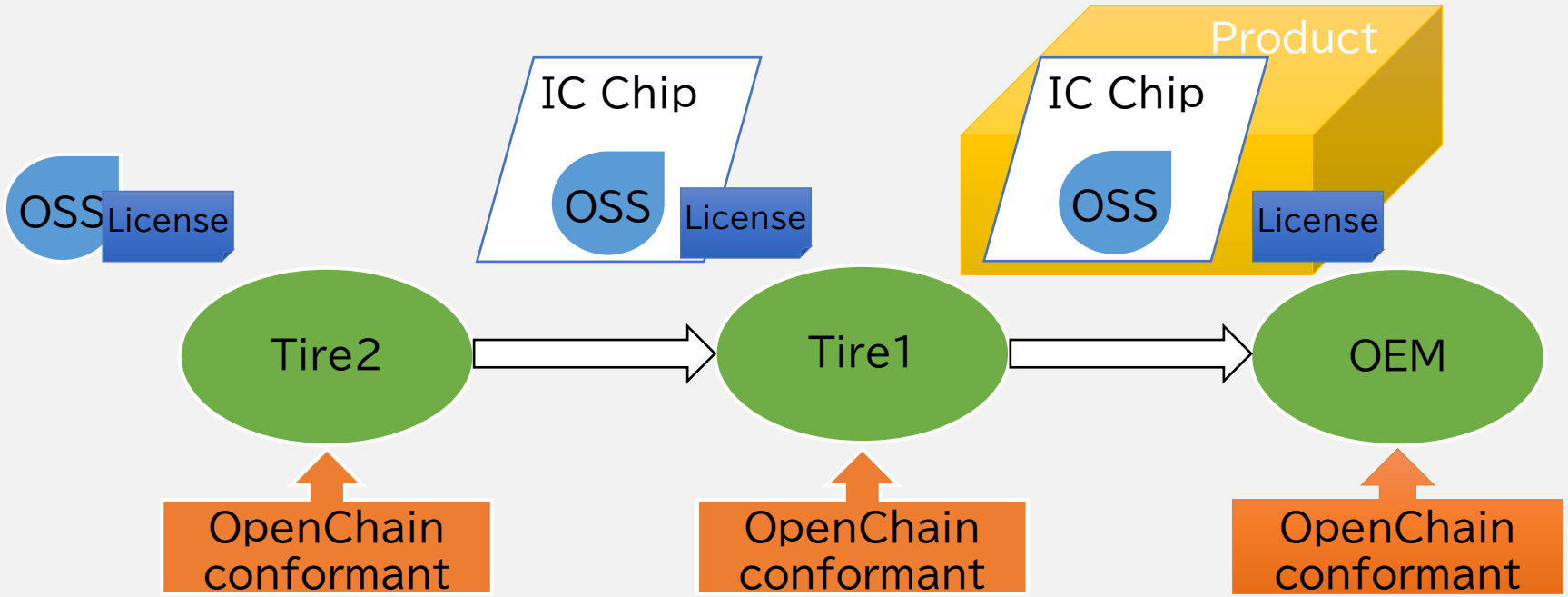
What is OpenChain?

- OpenChain is one of The Linux Foundation's official projects to develop standard of OSS license compliance.



Purpose Of OpenChain Project

- Establish compliance program requirements for each participant to establish within their organization to build trust throughout the OSS supply chain.
- Also, a community was formed to share educational materials and best practices from each company



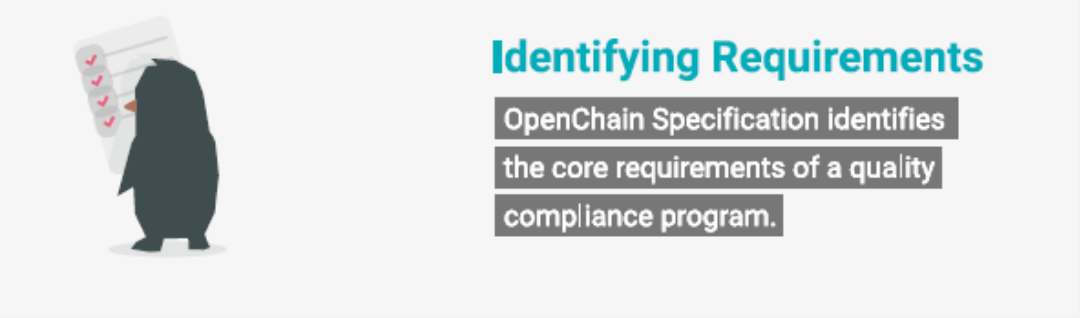
Platinum Members

https://openchainproject.org/community

3 Major outputs of OpenChain

Specification

The OpenChain Specification defines a core set of requirements every quality compliance program must satisfy.

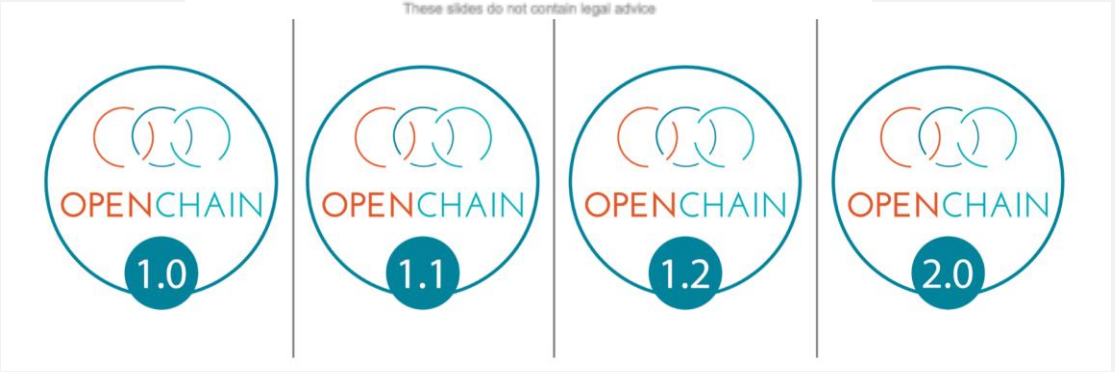


Curriculum

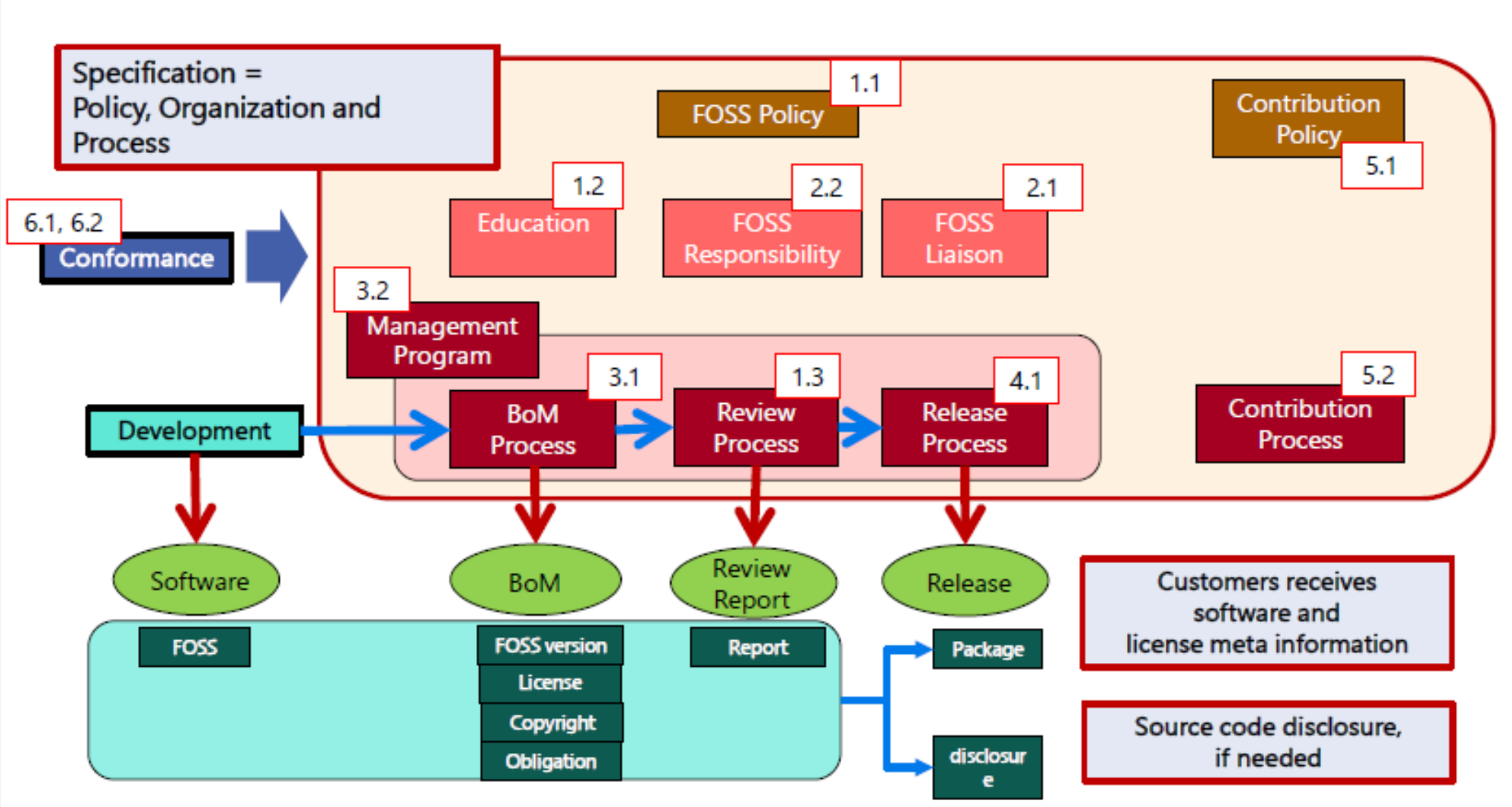
The OpenChain Curriculum provides the educational foundation for open source processes and solutions, whilst meeting a key requirement of the OpenChain Specification.

Conformance

OpenChain Conformance allows organizations to display their adherence to these requirements.

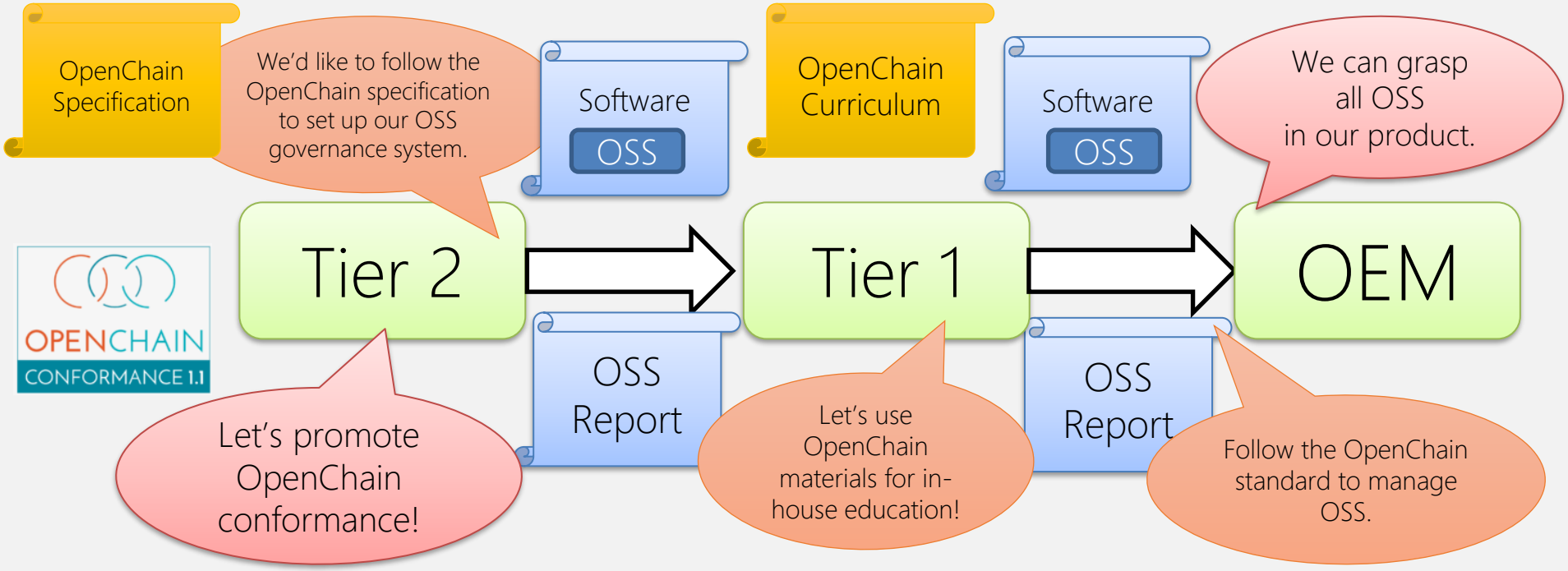


OpenChain Spacification



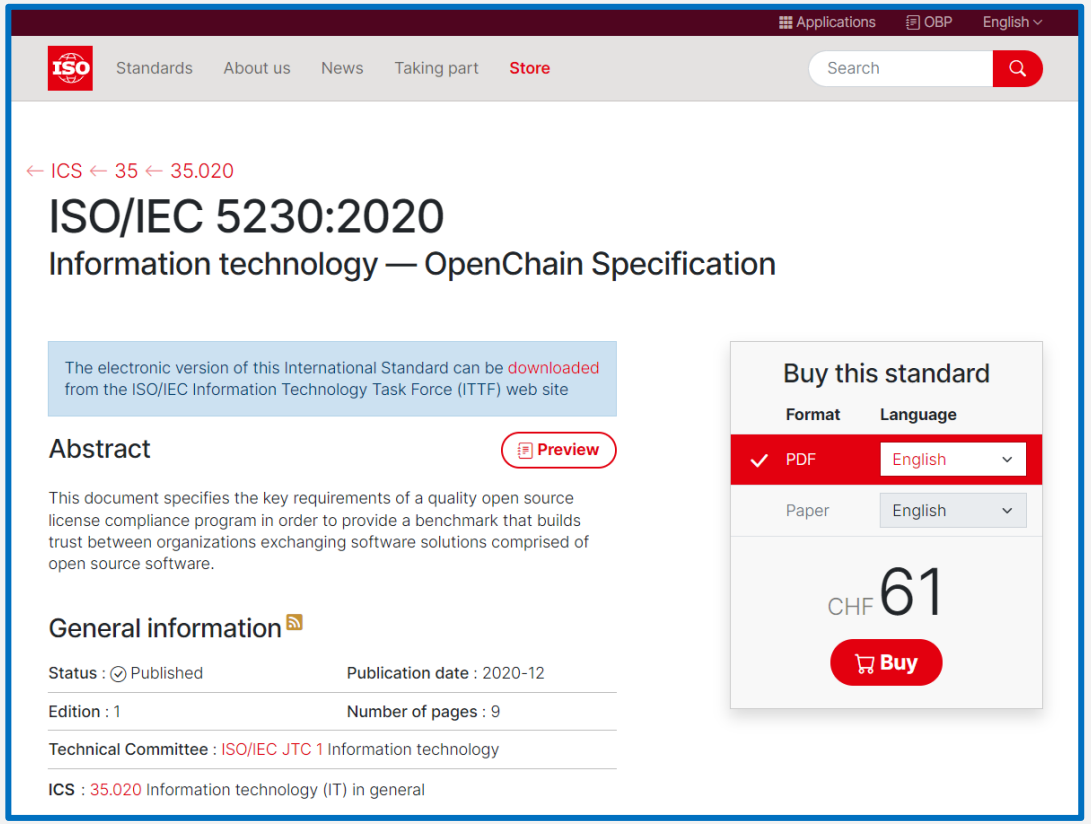
Pros of applying OpenChain to the Supply Chain

- OpenChain materials will provide strong OSS governance throughout the whole supply chain.

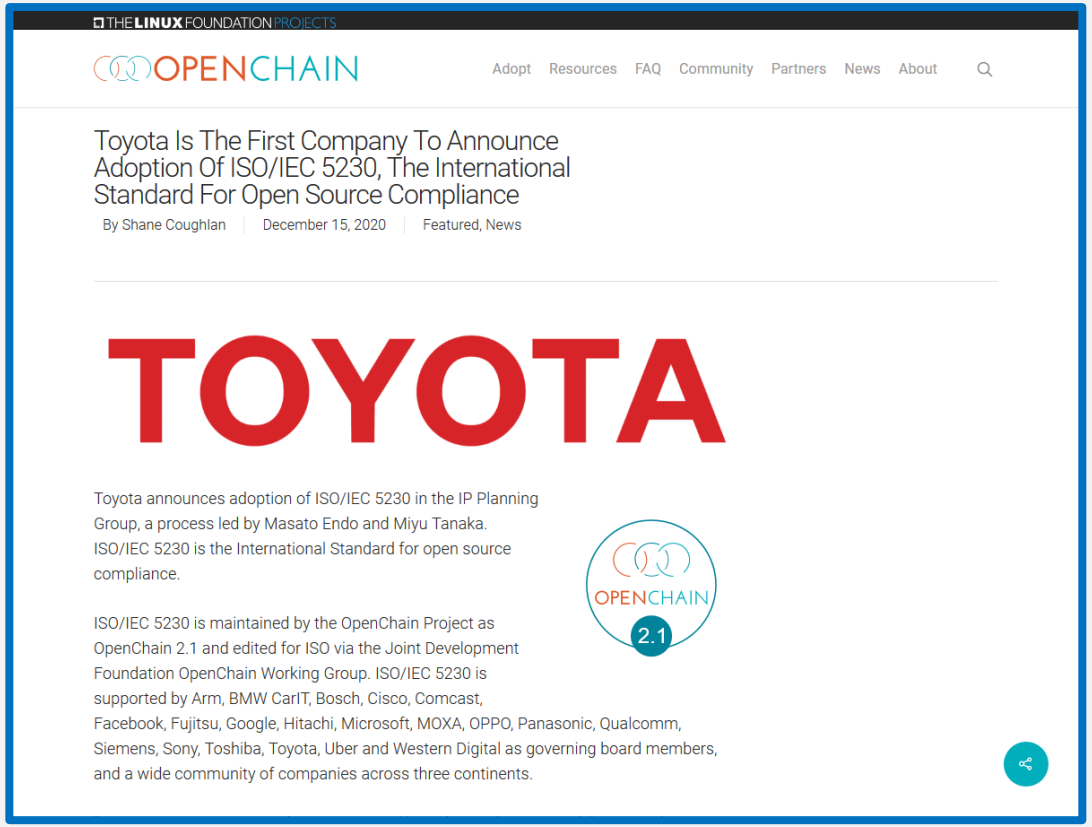


OpenChain Spec. 2.1 >> ISO/IEC 5230:2020

- The OpenChain standard will become an international standard in 2020 as ISO/IEC 5230:2020.
- Toyota is the first company to publicly announce its compliance with the standard.



https://www.iso.org/standard/81039.html



https://www.openchainproject.org/featured/2020/12/15/toyota-iso-5230

Companies with a Public OpenChain Conformant Program

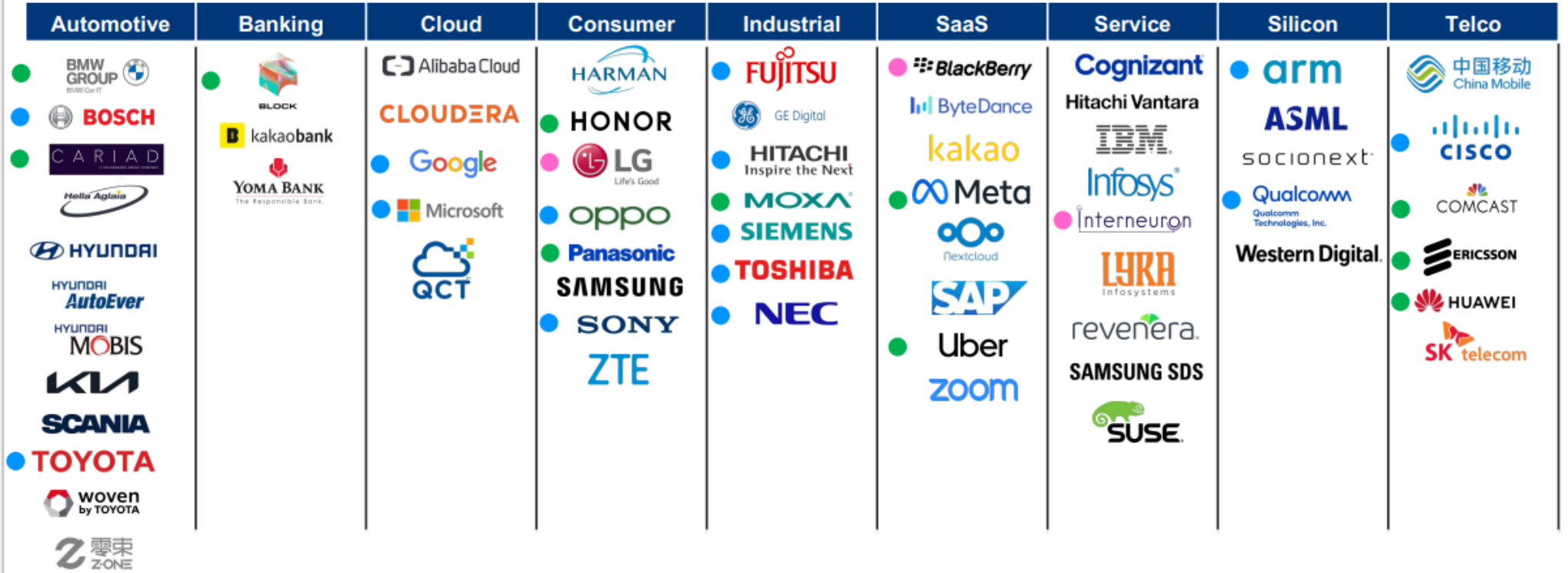
適合を宣言する組織

2020/12/01	トヨタ自動車	2021/09/07	Woven Planet	2022/04/06	TOSHIBA	2023/06/27	xFusion (100社目)	2024/05/13	Socionext (re-certification)
2020/12/15	NCSOFT	2021/09/08	Synology	2022/05/24	ZTE	2023/07/05	LINE	2024/07/09	IAV GmbH
2020/12/17	Cisco	2021/09/08	SK Telecom	2022/07/13	Samsung SDS	2023/07/27	Collabora	2024/07/24	dSPACE GmbH
2021/01/13	NTTデータ	2021/10/19	NEC	2022/08/01	KKCompany	2023/10/04	Bobble AI	2024/09/15	Nokia
2021/02/01	Microsoft	2021/12/15	ETRI	2022/08/16	Hyundai Motor Company	2023/11/02	Vectorverse	2024/09/17	OpenHarmony
2021/02/08	日立製作所	2022/01/24	Kakaobank	2022/08/16	Kia	2023/11/07	Korea Telecom	2024/10/16	Osaka NDS
2021/03/02	LG	2022/01/24	Kakao	2022/08/16	Hyundai Mobis	2023/11/12	LSware	2024/11/7	HARMAN International
2021/04/06	Nanjing Fujitsu Nanda Software Technology Co., Ltd.	2022/02/14	GBase 8a from General Data Technology Co., Ltd. (GBASE)	2022/08/16	Hyundai Autoever	2023/12/06	Honda	2024/12/4	HLB Surlatina Chile
2021/04/22	Keitaro	2022/02/14	KingbaseES V8 from CETC Kingbase	2022/11/04	NAVER	2024/01/12	Software Security Technology	2024/12/20	ETRI (re-certification)
2021/07/07	Samsung Electronics	2022/02/14	Tidb enterprise v4.0 from PingCap	2022/11/11	Fujitsu	2024/01/14	Shanghai Computer Software Technology Development Center	2024/12/20	AVL List GmbH
2021/07/13	Bosch	2022/03/17	BlackBerry	2022/12/06	Google	2024/01/30	CEHLabs	2025/1/20	KFTC
2021/08/09	Sony Semiconductor	2022/03/28	Revenera	2023/03/31	Socionext	2024/02/29	Circle	2025/2/1	Erlang/OTP Project
2021/08/19	QCT	2022/03/28	SAP	2023/Apr	China Mobile、Alibaba、Cloudera、SAIC X-ONE、ByteDance	2024/04/03	emlix		
2021/08/22	Coontec					2024/04/15	Volvo Cars		

https://www.openchainproject.org/news

Companies with a Public OpenChain Conformant Program

Example Verticals Impacted by OpenChain



● Platinum Member / Conformance Pending ● Platinum Member + ISO/IEC 5230 Conformant ● ISO/IEC 5230 + DIS 18974 Conformant

This is a snapshot based on membership and select conformant organizations currently listed on our website. Total conformant numbers are far higher.
Example: PwC Survey shows 20% of companies in Germany with over 2,000 employees already used ISO/IEC 5230.

OpenChain Japan WG

Hitachi, Sony and Toyota set up Japan WG in 2017.
Each Sub-WG makes materials for OSS compliance and uploads to GitHub.

SWG participants
Event speakers
~50 people

Bimonthly meeting
~100 people

ML subscribers
200+ people

SUB Working Groups

- -Planning SWG
- -FAQ SWG
- -Leaflet to Supplier SWG
- -Education material for roles SWG
- -License information exchange SWG
- -Tooling SWG
- -Promotion SWG

OPENCHAIN

OpenChain Automotive WG

Purpose

- Raise awareness about the importance of OSS compliance in the industry
- Share information to support best practices in the industry
- Build a future industry standard for OSS SCM

@Tokyo

@Lyon

@CES2020

@Stuttgart

SOAFEE

Thank You