Bosch OpenChain Conformity

Hans Malte Kern
Head of Bosch Center of Competence Open Source

BOSCH

Agenda

1. About Bosch
2. Compliance at Bosch
3. Open Source like a Bosch
4. Historical Milestones
5. Bosch Open Source Policy Implementation
6. Learnings from 8 years of Corporate Open Source Management

Bosch OpenChain Conformity
Who we are

Our ownership structure

The vast majority of company shares are held by Robert Bosch Stiftung GmbH, a charitable foundation, while the vast majority of voting rights are held by Robert Bosch Industrietreuhand KG, an industrial trust.

This special ownership structure serves to maintain founder Robert Bosch's tradition of civic engagement while also securing the company's strong and meaningful development.

Our business sectors

Mobility Solutions

Industrial Technology

Energy and Building Technology

Consumer Goods

Bosch OpenChain Conformity

Who we are

Our company in figures (in 2021)

78.5

billion euros
sales revenue

3.2

billion euros EBIT
from operations

403,000

Bosch associates
worldwide at year-end
(approx.)

~40,000
software developers

440

subsidiaries and
regional companies in
more than 60 countries

Bosch OpenChain Conformity

Who we are

Our company around the globe

Europe

52%
share of sales

41.3bn
sales revenue

246,000
associates (approx.)

Asia Pacific*

31%
share of sales

24.5bn
sales revenue

110,000
associates (approx.)

Americas

16%
share of sales

12.8bn
sales revenue

46,000
associates (approx.)

* including Africa

Bosch OpenChain Conformity
Compliance at Bosch

For Bosch Compliance matters:

- In our **Code of Business Conduct**, legal compliance is a core value

> "We adhere to the principle of legality in all dealings, actions, contracts, and other activities of the Bosch Group."

- This statement is no different for our Open Source activities and the expectation we build our supply chain upon.

- This was one reason why we joined the Linux Foundation's OpenChain Project in Feb 2019.

Bosch OpenChain Conformity
“Open Source like a Bosch”

- **We cover a range of Open Involvements**
  - We have different strategies and levels of involvement in Open Source, ranging from business that prohibits the use of Open Source to business that requires a full-fledged Open Source participation in an Open Source project.
  - *This range had to be addressed in our regulations*

- **We are a software integrator and “Tier-1”**
  - We have various software (and even hardware) suppliers that provide us with proprietary products that often contains Open Source or derivative works of Open Source. We integrate it into our products and distribute it to our customers.
  - *This requires contracting, trust and checks*

- **We have a variety of Products and Applications and Markets**
  - The final Open Source obligation fulfillment heavily depends on the product itself, the market, the distribution, the customer, the product stage ranging from innovation to commodity.
  - *This leads to often-unique approaches on how we fulfill license obligations*

Bosch OpenChain Conformity
Historical Milestones

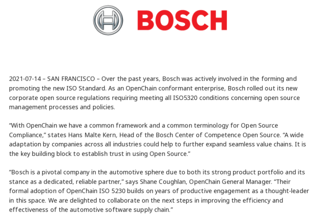
2014/10
First Corporate Directive (CD 1.0)
Heavily influenced by legal and difficult for developers to implement.

2015/12
Fist reflection (CD 2.0)
Brought both worlds together, legal and developers were satisfied and enabled

2019/02
Bosch joins OpenChain

2020/12
OpenChain2.1 – ISO/IEC 5230 released

2021/01
OpenChain conform regulations (CD 3.0)
Roll-Out started, only minor changes were necessary.



2021-07-14 – SAN FRANCISCO – Over the past years, Bosch was actively involved in the forming and promoting the new ISO Standard. As an OpenChain conformant enterprise, Bosch rolled out its new corporate open source regulations requiring meeting all ISO5320 conditions concerning open source management processes and policies.

“With OpenChain we have a common framework and a common terminology for Open Source Compliance,” states Hans Malte Kern, Head of the Bosch Center of Competence Open Source. “A wide adaptation by companies across all industries could help to further expand seamless value chains. It is the key building block to establish trust in using Open Source.”

“Bosch is a pivotal company in the automotive sphere due to both its strong product portfolio and its stance as a dedicated, reliable partner,” says Shane Coughlan, OpenChain General Manager. “Their formal adoption of OpenChain ISO 5230 builds on years of productive engagement as a thought-leader in this space. We are delighted to collaborate on the next steps in improving the efficiency and effectiveness of the automotive software supply chain.”

2021/07
Corporate OpenChain Conformity Announcement

2022/01
CD 3.1
Process improvements

2022

Bosch OpenChain Conformity

Conformity Announcement

2021-07-14 – SAN FRANCISCO – Over the past years, Bosch was actively involved in the forming and promoting the new ISO Standard. As an OpenChain conformant enterprise, Bosch rolled out its new corporate open source regulations requiring meeting all ISO5320 conditions concerning open source management processes and policies.

“With OpenChain we have a common framework and a common terminology for Open Source Compliance,” states Hans Malte Kern, Head of the Bosch Center of Competence Open Source. “A wide adaptation by companies across all industries could help to further expand seamless value chains. It is the key building block to establish trust in using Open Source.”

“Bosch is a pivotal company in the automotive sphere due to both its strong product portfolio and its stance as a dedicated, reliable partner,” says Shane Coughlan, OpenChain General Manager. “Their formal adoption of OpenChain ISO 5230 builds on years of productive engagement as a thought-leader in this space. We are delighted to collaborate on the next steps in improving the efficiency and effectiveness of the automotive software supply chain.”

https://www.openchainproject.org/featured/2021/07/13/bosch-iso-conformance

Bosch OpenChain Conformity
Bosch Open Source Policy Implementation

Governance

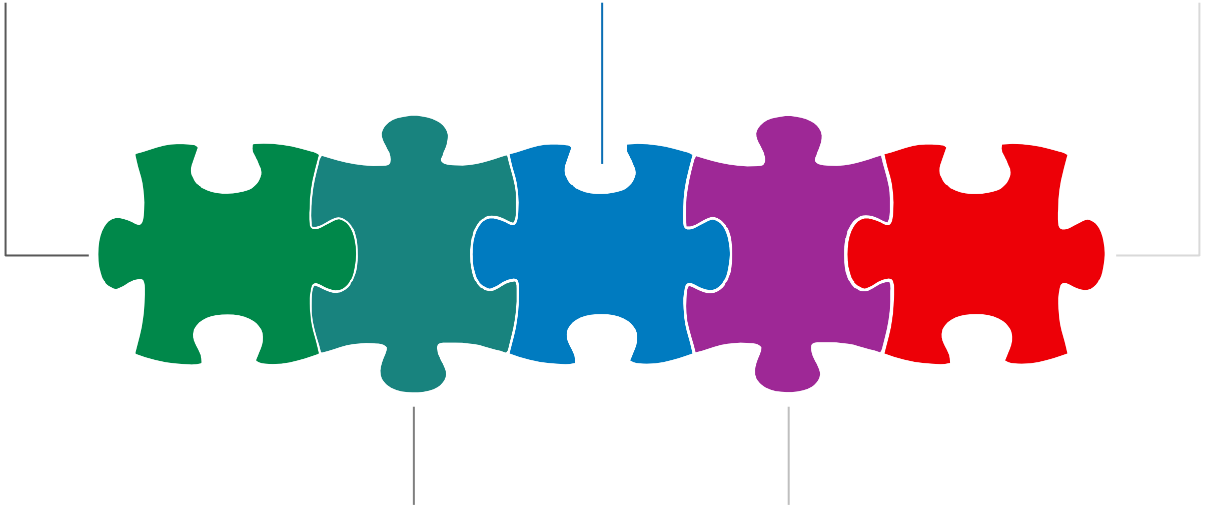
Direct Compliance Hotmail access, internal and supplier audits ensure governance

License compliance

Understanding OSS Licenses and its implications, that is what matters

Documentation

Solid Open Source Compliance comes with structured documentation



Training

Not all employees must have the same knowledge, instead tailored trainings are offered

Processes

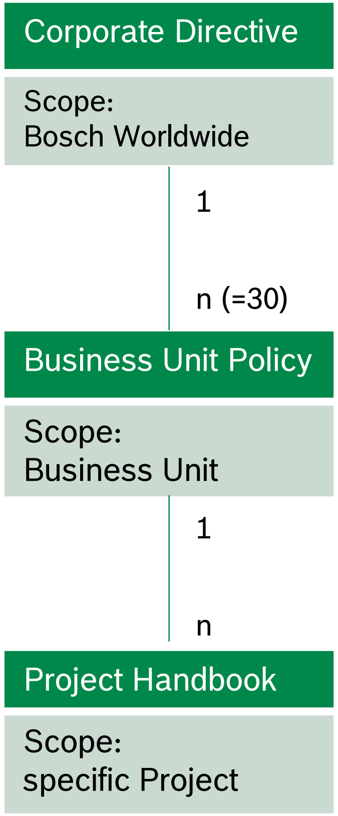
What processes are valid, where to find the processes, and what do the processes govern

Bosch OpenChain Conformity
Governance: Regulations & Policies

- Corporate Directive Open Source
  - describes mandatory compliance requirements and mandatory processes
  - provides good practices
  - covers all requirements from ISO/IEC 5230:2020 in a way that satisfy our “way of doing”

- Business Unit Open Source Policy
  - implements the Corporate Directive Open Source on Business Unit level
  - is mandatory regulation on Business Unit level

- Project Handbook
  - “is a running instantiation of the Business Unit Open Source Policy and binding for the project”


Corporate Directive

Scope:
Bosch Worldwide

1

n (=30)

Business Unit Policy

Scope:
Business Unit

1

n

Project Handbook

Scope:
specific Project

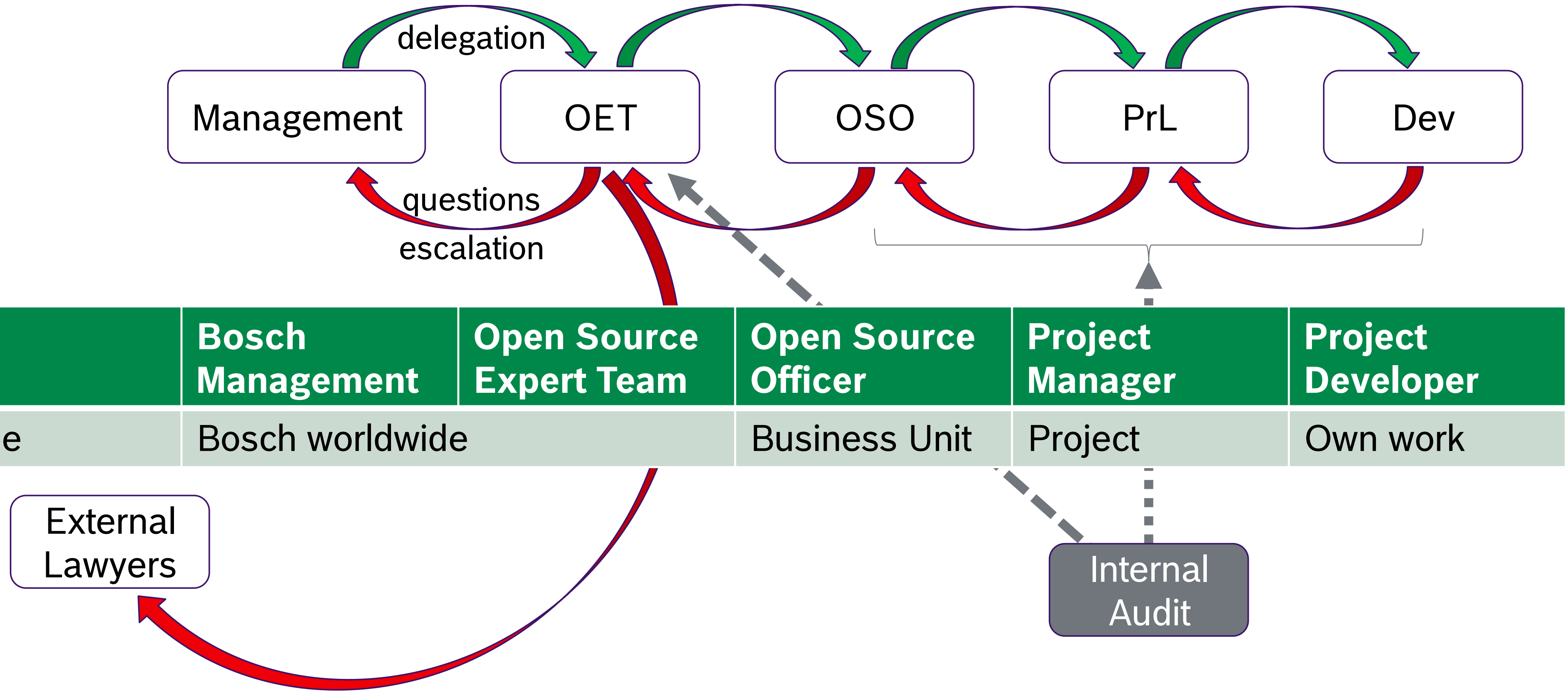
Bosch OpenChain Conformity
Governance: People and Roles

- The mandate for Corporate Open Source Governance is with the **Open Source Expert Team**, which consists of legal and technical employees.
- Every organizational entity has its own **Open Source Officer** who is taking care of the Open Source Governance.
- The **Center of Competence Open Source** is the hub for all Open Source topics and consists of
    - Open Source Expert Team
    - all Open Source Officers
    - OSS experts
  - It covers governance, training & awareness, tooling and OSS strategy.
- In addition, there are internal OSS Service Offerings, like
    - Central provisioning of standardized Open Source management tools
    - Open Source Management service
    - Open Source Scan service

Bosch OpenChain Conformity

Governance: Governance and Escalation Cascade

Governance



	Bosch Management	Open Source Expert Team	Open Source Officer	Project Manager	Project Developer
Scope	Bosch worldwide		Business Unit	Project	Own work

Governance

Bosch OpenChain Conformity
Governance: Standardized Terms & Conditions

- Terms & Conditions for handling Open Source in the “inbound” were standardized and incorporated in our contractual basis for the cooperation between Bosch and partners
  - ~ 1400 words legalese only for OSS, to
  - Ensure Open Source compliance in the supply chain towards us, and
  - Enables us to fulfill supplied Open Source license obligations towards our customers

  - Purchasing Terms and Conditions
    - https://www.bosch.com/company/supply-chain/information-for-business-partners/#purchasing-terms-and-conditions

What if OpenChain publishes standardized T&C to speed-up any negotiations.
This would also allow us to have a common understanding.

Bosch OpenChain Conformity
Training

- Corporate wide curriculum with mandatory and optional trainings ensures that every employee will get the correct training and the participation is documented in the employee’s training history
- Different trainings, all maintained by the Center of Competence
  - Mandatory for all developers: Basic Open Source Awareness
  - Mandatory for developers working with OSS, Sales and Purchase: Advanced OSS
  - Open Source Officers and their deputies: Open Source Officer Training
  - Contributors: Contribution Training
  - OE specific Basic trainings, e.g. OSS Deny Training
  - Tool Trainings
- For suppliers and external developers, we refer to the free training offered by Linux Foundation
  - especially to “LFC193 – Introduction to Open Source License Compliance Management“

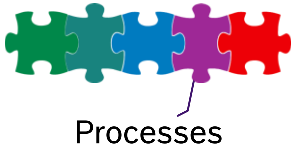
Bosch OpenChain Conformity
License Compliance

"This leads to often-unique approaches on how we fulfill license obligations"

- We have a corporate evaluation of Open Source licenses – License Master List
  - It is a collection of our previous legal and technical evaluations of Open Source licenses
  - Provides for various use and distribution cases the way how we fulfill Open Source license obligations

- Issues we have
  - License Mapping
    - with SPDX we have a unique ID, but not for all licenses
    - and sometimes a developer changes a license a bit and we must evaluate the "new license"
  - Lack of copyright awareness in the OSS world: IMPI -- incomplete / missing / partially / ignored licenses

Bosch OpenChain Conformity
Processes



- **Deny**

  Clear process, tool and documentation requirements for project that follow a “deny strategy” (most often imposed by customer).
- **Use**

  Process, documentation and license fulfillment regulated to ensure license compliance. More freedom to chose the tool that fits best to the development style.
- **Contribution**

  Corporate wide unified process that provides accelerations for “uncritical” contributions, up to a check for IP risks that will produce an answer within 14 days.
- **Champion**

  Process, similar to Contribution that enables us to take over the responsibility for an Open Source project or to start one.
- **Board Membership**

  Process, that enables us to participate in the Board of an Open Source organization in alignment with our strategies.

Bosch OpenChain Conformity
Documentation

Documentation

- **(internal) OSS Review Documentation**
  Written proof of performed Open Source Management as required by our policies, such as the OSS Scan Report and its review. It also contains the approval for using the OSS Components.
- **(external) OSS Compliance Bundle**

  OSS Compliance Bundle is a set of artifacts that represent the information which must be distribute with the product to the customer. It includes, depending on the applicable OSS Licenses, among others: attribution notices, source code, build and install scripts, license texts, copyright notices, modification notifications, or written offers.

We have for each automotive OEM a different template for their OSS Compliance Bundle. Each has its own format and following its own approval processes.

Current version of SPDX is not sufficient to solve this issue, but it would be a first unification step!

Bosch OpenChain Conformity
Bosch Open Source Policy Implementation

Processes

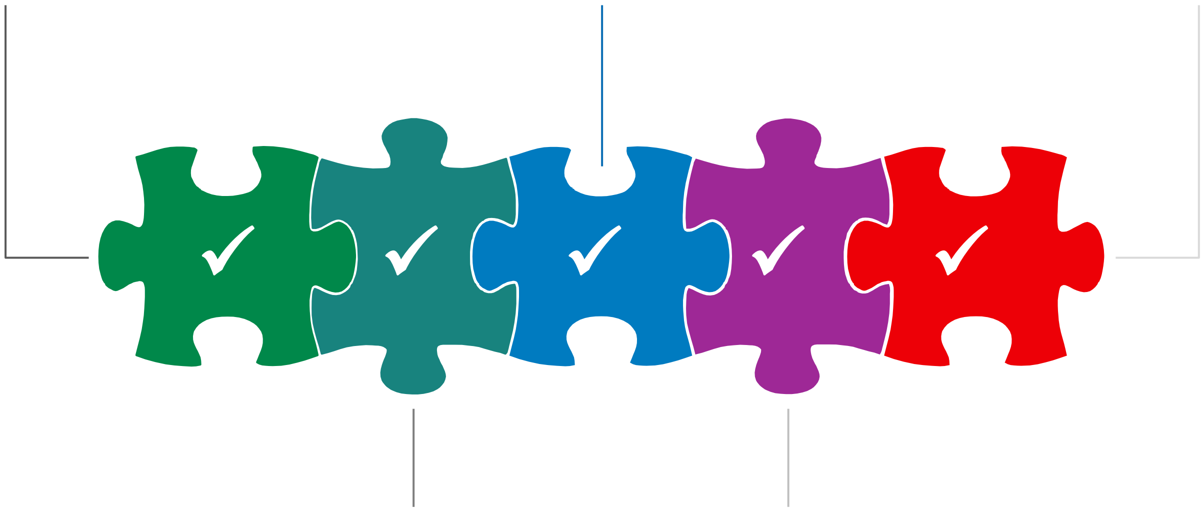
What processes are valid, where to find the processes, and what do the processes govern

License compliance

Understanding OSS Licenses and its implications, that is what matters

Documentation

Solid Open Source Compliance comes with structured documentation



Training

Not all employees must have the same knowledge, instead tailored trainings are offered

Governance

Direct Compliance Hotmail access, internal and supplier audits ensure governance

Bosch OpenChain Conformity

Learnings from 8 years of Corporate Open Source Management

- Open Source Management is always a Joint-Adventure between development and legal.
- Open Source is still a FUD (Fear, Uncertainty, and Doubt) topic, and we had to take away this fear from our suppliers and customers.
- We often had to educate our suppliers why Open Source management is important, and we hope that the ISO 5230 makes a difference.
- Introducing tooling drastically changed how we deal in Open Source.
- The legal frameworks (licenses, CLAs) became heavier and also more important.
- Defining success for an Open Source participation require different evaluation methods and a new management culture.

THANK YOU!