How do I trust my open source supply chain?
The Companies behind OpenChain

Adobe  arm  Bosch  Cisco  Comcast
Facebook  Fujitsu  Google  Hitachi  Microsoft
Panasonic  Qualcomm  Siemens  Sony  Toshiba
Toyota  Uber  Western Digital
The OpenChain Project defines the key requirements of a quality open source compliance program.
OpenChain Defines Inflection Points

upstream \[\rightarrow\] inbound \[\rightarrow\] Training Policy Process \[\rightarrow\] outbound \[\rightarrow\] downstream
Result: Predictable B2B Compliance Activity
# Our Online Self-Certification Questionnaire

<table>
<thead>
<tr>
<th>Question</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>G1: Know Your Open Source Responsibilities</strong></td>
<td>0 out of 12</td>
</tr>
<tr>
<td><strong>G2: Assign Responsibility for Achieving Compliance</strong></td>
<td>0 out of 8</td>
</tr>
<tr>
<td><strong>G3: Review and Approve Open Source Content</strong></td>
<td>0 out of 8</td>
</tr>
<tr>
<td><strong>G4: Deliver Open Source Compliance Artifacts</strong></td>
<td>0 out of 3</td>
</tr>
<tr>
<td>- Do you have a documented procedure that describes a process that ensures the Compliance Artifacts are distributed with Supplied Software as required by the Identified Licenses?</td>
<td></td>
</tr>
<tr>
<td>- Do you archive copies of the Compliance Artifacts of the Supplied Software?</td>
<td></td>
</tr>
<tr>
<td>- Are the copies of the Compliance Artifacts archived for at least as long as the Supplied Software is offered or as required by the Identified Licenses (whichever is longer)?</td>
<td></td>
</tr>
<tr>
<td><strong>G5: Understanding Open Source Community Engagements</strong></td>
<td>0 out of 3</td>
</tr>
<tr>
<td><strong>G6: Adherence to the Specification Requirements</strong></td>
<td>0 out of 2</td>
</tr>
</tbody>
</table>
A Simple Logo, A Significant Meaning

Quality Open Source Compliance Defined
Publicly Announced OpenChain Conformant Programs
Interneuron
Interneuron’s Approach to Open Source Compliance Management in Health Tech

Interneuron is a Community Interest Company (CIC) in the U.K. focused on building, developing, and deploying software specifically for the healthcare IT industry. The company’s singular focus is creating high-value software applications that serve the best interest of patients in need of health and social care services.

ORGANIZATIONS:
- Community Interest Company (CIC) – a Not for profit
- Focused on building, developing, and deploying software specifically for the healthcare IT industry
- Everything developed by Interneuron will be open source and is specified in their articles of association

CHALLENGES:
- Overcoming perception that traditional proprietary software is the least risky option
- Enable 100% transparency of the use of third-party open source
- Decrease the knowledge gap around measuring open source quality and effectiveness including IP and security

SOLUTION:
- Building oversight and governance by design
- Empowering and motivating developers to be responsible for complying with company guidelines
- Education – Company wide knowledge sharing of controlled used of open source
- Secure license obligations

BENEFITS:
- Transparent demonstration of quality assurance; unachievable by proprietary solutions
- Automated tracking third party open source software components for both licensing and security vulnerabilities
- Decreased patent and licensing risks
OpenChain in Japan
OpenChain in Japan (Dec 2017~)

Meeting attendee

- Num. of attendees
- Num. of entities

Ad Hoc Meeting
OpenChain in Japan (2x in 2019)
OpenChain in Korea (Jan 2019~)

Meeting 1: 26 Attendees @ LGE
Meeting 2: 31 Attendees @ Samsung
Meeting 3: Sept 4th @ SK Telecom
OpenChain in India (Sept 2019~)

Meeting 1: Sept 7 @ SFLC.in
OpenChain in China (Sept 2019~)

Meeting 1: Sept 25 @ Huawei
OpenChain in Taiwan (Sept 2019~)

Meeting 2: Sept 27 @ Open Culture Foundation
Automotive Work Group (July 2019~)

The Automotive Work Group started with 95 participants.

- Share information to support best practices in the industry
- Build a future industry standard for Open Source Software Supply Chain Management (OSS SCM)
- Raise awareness about the importance of open source compliance in the industry

https://groups.io/g/openchain-automotive-work-group/topics
Automotive Work Group - Diversity

Volkswagen
Toyota
Suzuki
Scania
Hyundai
Honda
Subaru
Isuzu
Mazda
GM
Porsche
Renasas
Hitachi
Panasonic
Pioneer
Denso
Denso Ten
LGE
Uber
HELLEA
Bosch SI
Elektrobit
TRI-AD
Mitsubishi Electric
Qualcomm
Fujitsu
TUV SUD
+ More
OpenChain in ISO (June 2019~)

The OpenChain Project is submitting our specification to ISO via Publicly Available Specification (PAS) in Joint Technical Committee 1 (JTC-1).

Working in partnership with Joint Development Foundation we expect to become a formal standard in the 1st half of 2020.
Partner Program (2x in 2019)
Partner Program – Newest Participant
Third Party Certification in Japan (Nov 2018~)
Global Third Party Certification (Mar 2019~)

http://shorturl.at/hpsP7
OpenChain 3rd Party Certification

ORGANIZATION:
TÜV SÜD is a provider of testing, inspection and certification services based in Germany with subsidiaries in all major industries.

CHALLENGES:
1. OpenChain is an established and growing de-facto industry standard but not yet an official one as of 2H 2019. OpenChain expects to become an ISO standard in 2020.
2. While there are comprehensive

SOLUTION:
1. TÜV SÜD addresses the above challenges by creating testing methods based on OpenChain that meet the requirements of 3rd party certification.
2. Adjacent to this TÜV SÜD has created a test mark and

BENEFITS:
1. The results of the independent TÜV SÜD assessment can serve as evidence for an appropriate compliance system in case of dispute.
2. The assessment can also provide a competitive
Freedom of Choice for Customers and Suppliers

Self-Certification

Independent Compliance Assessment

Third Party Certification
OpenChain is run by user companies for user companies.
Be Part of This

Join the community: https://www.openchainproject.org/community

Self-Certify or Health Check an organization: https://certification.openchainproject.org