



OPENCHAIN

Annual Report

2023


Welcome to the OpenChain Annual Report for 2023

The work of the OpenChain Project is made possible by our Platinum Members. In 2023, our Governing Board helped guide the project in meaningful ways towards improving legal and security challenges in the global supply chain. I would like to thank everyone involved in providing this strategic and financial support, with special thanks to Jimmy Ahlberg from Ericsson who acted as Chair, and to the formal voting representatives of our 2023 Platinum Member companies:





The result of their support was remarkable.

Summary



The key strategic goals identified by our governing board were met. Our message and our stage for delivery has grown in all directions.




1

The OpenChain Project had an exceptional year throughout 2023. The key milestone was the ISO submission and publication of [OpenChain ISO/IEC 18974:2023](#), the new International Standard for open source security assurance. This is the sister standard to [OpenChain ISO/IEC 5230:2020](#), the International Standard for open source license


compliance. It is the culmination of over 18 months of work from dozens of contributors, and has already seen adoption by companies like [KakaoBank](#), [LG Electronics](#) and [BlackBerry](#). For those curious, we used the [JTC-1 PAS Transposition Process](#) in collaboration with our partners at the [Joint Development Foundation](#) to take our pre-existing de-facto industry standard and convert it into a formal ISO standard. This is the same mechanism we used with OpenChain ISO/IEC 5230:2020.

More broadly, our market impact was positive in every direction. As a standards project, the key things we look for are positive growth in terms of adoption, positive growth in our collaborative community and its activity, and positive growth in our partner ecosystem for officially endorsed support.

Global Impact Q1 to Q4 2023


OPENCHAIN

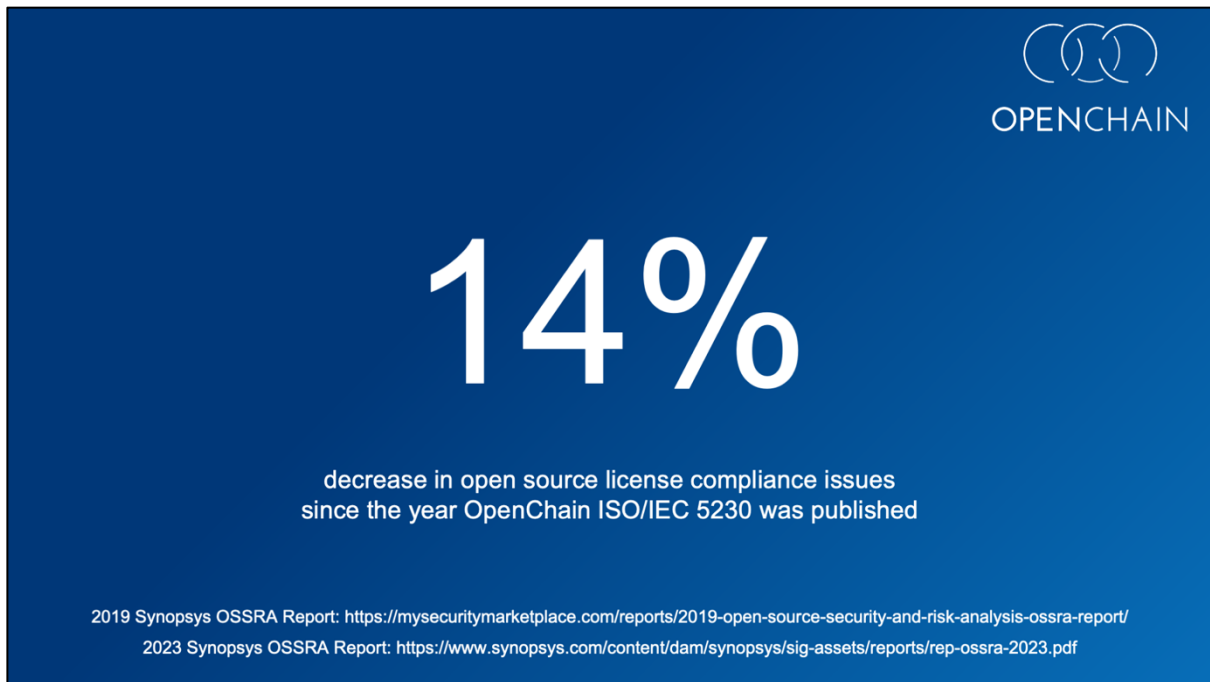
- ISO/IEC 5230 Conformant Programs Listed: 89 > 109 (22.48% increase)
- ISO/IEC 18974 Conformant Programs Listed: 1 > 6 (500% increase)
- Official Partner Third-Party Certifiers: 7 > 14 (100% increase)
- Official Partner Service Providers: 24 > 30 (25% increase)
- Official Partner Tooling Vendors: 11 > 13 (18.2% increase)
- Official Partner Legal Providers: 21 > 24 (14.3% increase)
- Standards maintained: 1 > 2 (100% increase)
- New specifications under proposal: 1 > 3 (200% increase)



Please note: Actual market conformance higher than "Conformance Listed" on our website.
"Conformance Listed" means they came to us and asked to be added to the website.

A tangible metric for our success is related to how many programs we are aware of around the world using one or both of the standards we currently publish. One way we track this is through asking companies to inform us of their use, and to allow us to add them to our '[Community of Conformance](#)' web page. In 2023, we crossed over 100 listings for ISO/IEC 5230 conformant programs on that page.

had license compliance issues. Three years later, that number standards at 54%, a 14% decrease in license issues impacting the business domain.



OpenChain ISO/IEC 18974 is at a much earlier stage in its market lifecycle. As with OpenChain ISO/IEC 5230, we expect it to take a while for companies to complete their adoption in security programs, but we already see the type of large and small entity early adoption that is a positive indicator for market fit. With a long and complex supply chain, it is vital to ensure that small companies, or companies with limited resources, can adopt our process management standards as easily as companies with sophisticated and well-funded teams.

ISO/IEC 18974 Conformant Programs Advertised



 **kakaobank**  **LG**
Life's Good

 **BlackBerry**  **CANOPUS**
Global Business Services

 **Interneuron**  **revenera**TM



In the context of the OpenChain Project, we primarily build and support our standards through an active user community. However, it is also extremely important to have a healthy adjacent ecosystem of commercial service providers to ensure supply chain participants can get help when needed. The OpenChain Project has an official partner program designed to promote commercial providers that work with us on messaging, outreach and broader community development. This ecosystem saw growth in every direction in 2023, most notably in doubling the number of third-party certifiers available across the global market.

14 Official Third-Party Certifiers (+7)



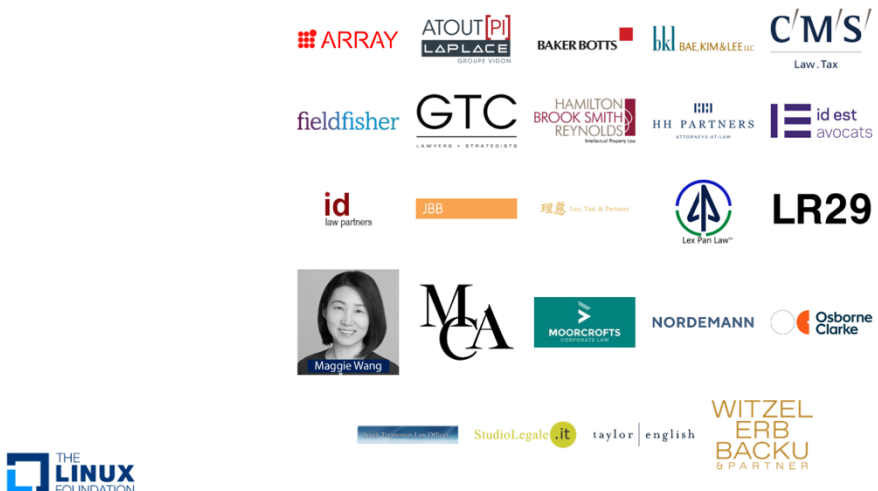
13 Official Tooling Vendors (+2)



30 Official Service Providers (+6)



24 Official Legal Providers (+3)



As the OpenChain Project enters 2024, we remain committed to the concept of measured, effective engagement with the global supply chain to promote adoption of our standards. A significant portion of our energy will be focused on this, both in the sense of directed project resources, and the expected outcomes of the collaborative user community and the commercial partner community.

The obvious starting point for all interested parties (and your supply chain) is to check out our resources to help companies adopt our standards through free self-certification, independent assessment or third-party certification.

Get Started with all our published standards:

- <https://www.openchainproject.org/get-started>

Learn more about OpenChain ISO/IEC 18974:2023 (security assurance):

- <https://www.openchainproject.org/security-assurance>

Learn more about OpenChain ISO/IEC 5230:2020 (license compliance):

- <https://www.openchainproject.org/license-compliance>

Naturally, the OpenChain Project is not static and our work is designed to evolve with the market. We invite all parties to help with collaborating around future updates to our business process standards for compliance, to help with developing new reference material or case studies and to explore the potential for new sister standards that support our mission.

For example, in the next few weeks we will launch an AI Study Group to assess the key metrics needed for compliance in this domain in the context of the supply chain. You can keep an eye out for that via our [newly created AI Study Group mailing list](#) and by reviewing the [recording of their first planning meeting](#).

When it comes to our existing standards, there are ongoing editing cycles for ISO/IEC 5230 (license compliance) and ISO/IEC 18974 (security assurance). The OpenChain Steering Committee took a look at the community developments in December 2023, and provided guidance that:

- The community-developed update proposals seem reasonable
- We will extend our Public Comment and Freeze Periods significantly to ensure the supply chain has time to consider the proposed changes
- The Public Comment period will change from 30 days to 6 months
- The Freeze Period will change from 14 days to 3 months
- This will be communicated in an [update to FAQ](#) and to our Specification Work Team.
- In principle, it is suggested that we target updates to our ISO standards once every five years
- This would suggest the update for ISO/IEC 5230 is likely to be ready for 2025
- ISO/IEC 18974 may be updated sooner due to a rapidly-moving market, but not at a speed that would hinder adoption of the existing and newly published version

Everyone is welcome to be part of this process.

License Compliance - Current and Draft Versions



Licensing Specification (CURRENT VERSION, 2nd Generation):

<https://github.com/OpenChain-Project/License-Compliance-Specification/blob/master/2.1/en/openchainspec-2.1.md>

Licensing Specification (3rd Generation Draft):

<https://github.com/OpenChain-Project/License-Compliance-Specification/blob/master/Official/en/3.0/openchain-license-compliance-3.0.md>

QR code is for the 3rd Generation Draft:



Security Assurance - Current and Draft Versions



Security Specification (CURRENT VERSION, 1st Generation):

<https://github.com/OpenChain-Project/Security-Assurance-Specification/blob/main/Security-Assurance-Specification/1.1/en/openchain-security-specification-1.1.md>

Security Specification (2nd Generation Draft):

<https://github.com/OpenChain-Project/Security-Assurance-Specification/blob/main/Security-Assurance-Specification/2.0/en/openchain-security-specification-2.0.md>

QR code is for the 2nd Generation Draft:



We look forward to an excellent 2024 in collaboration with you.

Shane Coughlan
OpenChain General Manager
4th January 2024