The OpenChain Project

Creating And Maintaining Standards For A Trusted Open Source Supply Chain

THE LINUX FOUNDATION

OPENCHAIN

OPENCHAIN

Global Codebase Statistics

Over 93% use open source

53% have license compliance issues

81% have security issues

https://www.synopsys.com/blogs/software-security/open-source-trends-ossra-report/ (2022)

Key News Around ISO/IEC 5230:2020

THE LINUX FOUNDATION

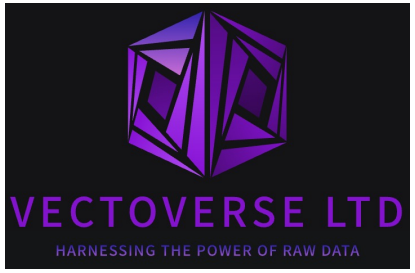
OPENCHAIN

OpenChain Has 108 ISO/IEC 5230 Conformant Orgs Listed On Our Website (totals are higher)

Total conformant numbers far higher.
Example: PwC Survey shows 31% of large companies in Germany use or are planning to adopt ISO/IEC 5230.

Recent ISO/IEC 5230 Conformance

OPENCHAIN



OPENCHAIN

12%

decrease in open source license compliance issues
since the year OpenChain ISO/IEC 5230 was published

https://www.synopsys.com/blogs/software-security/open-source-trends-ossra-report/ (2022)

31%

of large German companies already use or plan to adopt OpenChain ISO/IEC 5230

https://www.pwc.de/en/digitale-transformation/open-source-software-management-and-compliance/open-source-software-current-trends-and-developments.html

Key News Around ISO/IEC 18974:2023

THE LINUX FOUNDATION

OPENCHAIN

Conformance Continues With De-Facto Standard

OPENCHAIN

LG

Life's Good

BlackBerry

CANOPUS

Global Business Services

Interneuron

revenera™

THE LINUX FOUNDATION

Key Developments

OPENCHAIN

- ISO/IEC 18974:2023 is scheduled to be published in November 2023
- A major Korean financial institute will be announcing adoption this month.

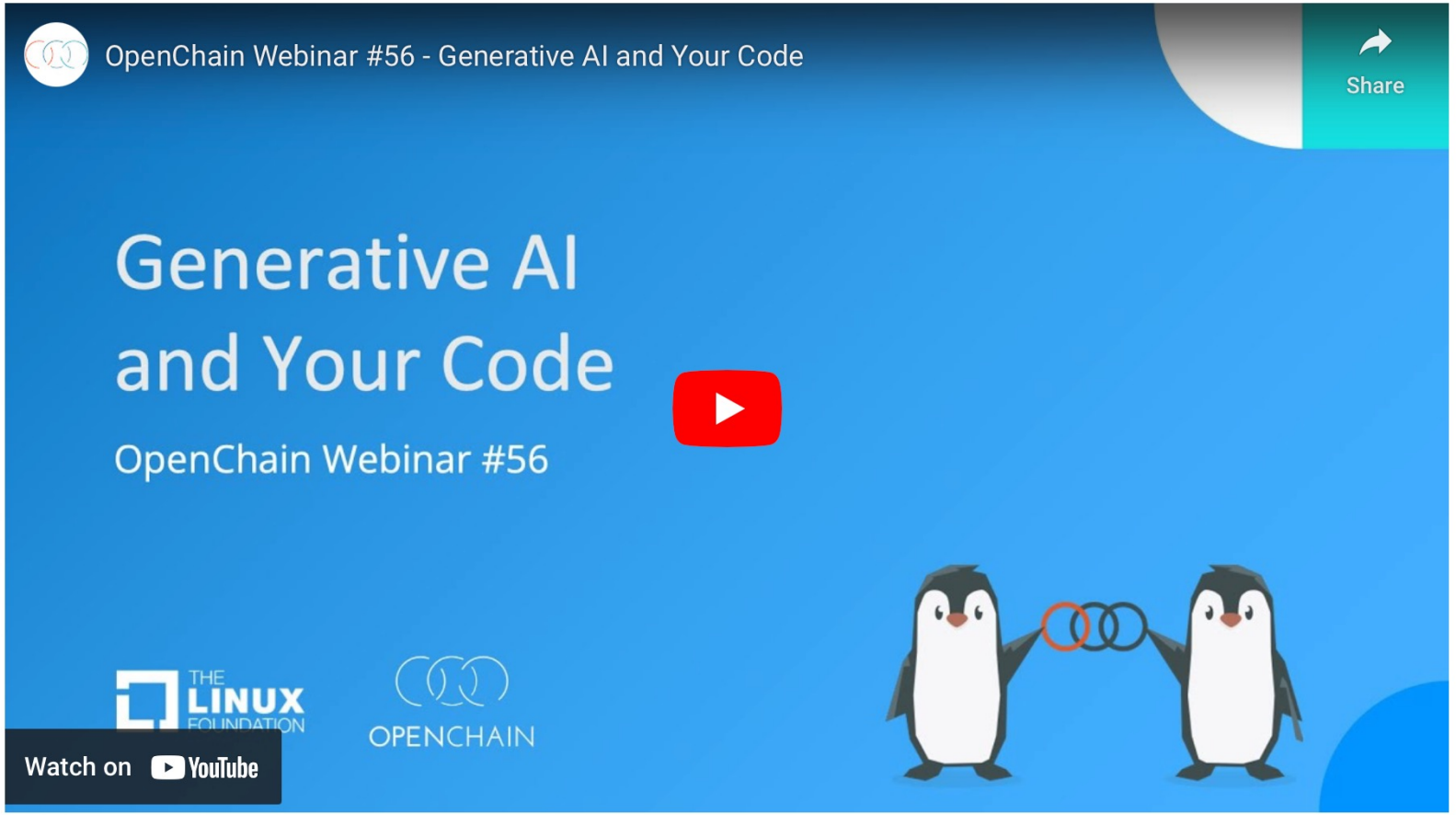
THE LINUX FOUNDATION

What Else Is Happening?

Continuing Our Educational Webinars

OPENCHAIN

Maximizing the Opportunity While Managing the Risks



This webinar had a poll about areas of interest around AI and law. Click here to access it.

https://www.openchainproject.org/featured/2023/09/14/webinar-56

Building The Future

The Headline

OPENCHAIN

With the acceptance of ISO/IEC 18974 by ISO, we maintain two ISO standards:

- ISO/IEC 5230 – open source license compliance process management
- ISO/IEC 18974 – open source security assurance process management

The OpenChain Project has evolved from credibility in *open source licence compliance process standardization* into having the ***ability*** to do various types of *open source business process standardization project*.

This has strategic implications.

- What do we do with our influence and potential?
- How do we ensure value for our board members?

Our mission remains building trust in the supply chain (reducing risk, saving money and time)

THE LINUX FOUNDATION

The Global Community Collaborates

- We are working on the ***proposals*** for:
  - OpenChain License Compliance 3.0 (ISO/IEC 5230:2020 next gen)
  - OpenChain Security Assurance 2.0 (ISO/IEC 18974:2023 next gen)
  - OpenChain Contribution Process Management 1.0 (name TBD)
  - OpenChain SBOM Quality Specification 1.0 (Telco Work Group)
- These will go before the OpenChain Steering Committee in early December for review.
- The Steering Committee will provide formal guidance on where to go next.

Current Versions of OpenChain Standards

Licensing Specification (CURRENT VERSION, 2nd Generation):

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

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

Draft Future Versions of Licensing / Security

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

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

Next Steps: Licensing / Security

OPENCHAIN

Open Issues

Both the next generation License Compliance specification and the next generation Security Assurance specification have pre-existing open issues for review:

- **Licensing:** https://github.com/OpenChain-Project/License-Compliance-Specification/issues/
- **Security:** https://github.com/OpenChain-Project/Security-Assurance-Specification/issues/

Proposed OpenChain Contribution Specification

- Contribution process community proposal – community editing underway: https://github.com/OpenChain-Project/Contribution-Process-Specification/blob/main/1.0/en/1.0.md

- First GitHub Issue: https://github.com/OpenChain-Project/Contribution-Process-Specification/issues/1

- Kick-Off Call: https://www.openchainproject.org/news/2023/08/23/contribution-spec-kick-off

SBOM Quality

- The OpenChain Telco Work Group has been working on a draft specification to describe a quality Software Bill of Materials: https://github.com/OpenChain-Project/Telco-WG/blob/main/OpenChain%20Telco%20SBOM%20Specification.md
- Everyone is welcome to open issues on GitHub for this: https://github.com/OpenChain-Project/Telco-WG/issues
- Please note: most of the discussion has happened on the Telco Work Group Mailing List, and they are currently discussing whether the draft spec should actually be an SPDX profile instead: https://lists.openchainproject.org/g/telco/messages

Track All This Work

- You can join our monthly North America / Europe and North America / Asia calls every month (two meetings per month): https://www.openchainproject.org/participate
- We publish the slides used for every meeting: https://github.com/OpenChain-Project/Meeting-Minutes/tree/main/Slides
- We also publish a recording of every meeting: https://www.openchainproject.org/news
- You can also join our specification mailing list to follow everything by email: https://lists.openchainproject.org/g/specification

tl;dr:

Big Project, Big Community.

Plenty Commercial Support Too.

THE LINUX FOUNDATION

OPENCHAIN

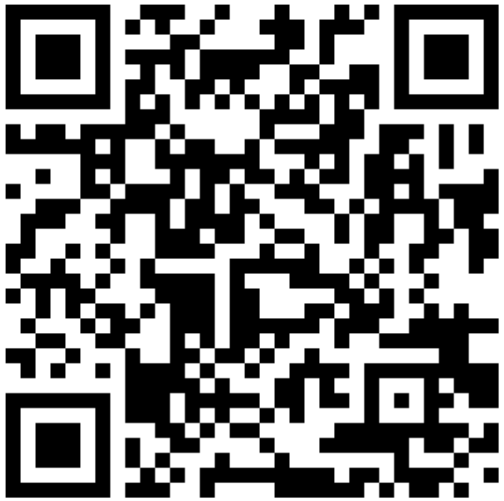
Global Impact January to October 2023

OPENCHAIN

- Conformant Companies Listed: 89 > 108 (20.3% increase)
- Certifiers: 7 > 13 (85.7% increase)
- Service Providers: 24 > 29 (20.8% increase)
- Vendors: 11 > 13 (18.2% increase)
- Legal Providers: 21 > 24 (14.3% increase)
- Standards maintained: 1 > 2 (100% increase)
- New specifications under proposal: 1 > 3 (200% increase)

THE LINUX FOUNDATION

Get Started With Your Adoption and Participation



https://www.openchainproject.org/participate