The new ISO 18974 – ISO 5230 as a stepping stone?

Katharina Grauf
BFOSS Erfurt, 27. September 2023
The new ISO 18974 – ISO 5230 as a stepping stone?
Introduction to ISO 18974*

Synergies of strategic ISO implementation

* "ISO 18974" is used in this presentation for the ISO/IEC DIS 18974 which will be released as an ISO soon. It is known as the OpenChain Security Assurance Specification 1.1., a de-facto industry standard.
1 Success Story
ISO 5230
→ just another compliance overhead?
Success story OpenChain ISO 5230

International standards increase transparency and build trust

- **International standard** for OSS license compliance (ISO 5230:2020)
- Offers established **best practices** and allows for flexible adoption
- **Increasing adoption** of ISO 5230 worldwide facilitating business operations
- **Risk mitigation** through increased transparency and control
- Streamlines OSS compliance and builds **trust in the software supply chain**
Success story OpenChain ISO 5230
International standards increase transparency and build trust

Facts and figures

Since the ISO 5230 has been released, the share of companies in Germany with OSS policies increased from 17% to **32%**.

**41%** of companies in Germany have established OSS compliance processes.

More than **100** conformance programs worldwide announced within the OpenChain Community.

Source: Bitkom e. V. Open Source Monitor 2023 (sneak preview results)
The ISO 5230 offers more than just license compliance

ISO 5230 adds value to the OSS ecosystem

- **Guidance** for implementation of OSPOs
- **Orientation** for active OSS practitioners
- **Proof of conformance** for mature OSS organisations

ISO 5230 enables…

- …development of *individual OSS strategy* and measures
- …realisation of *OSS advantages*
- …OSS license compliance to be thought of in *broader terms* and extended to the security environment
Introduction to ISO/IEC DIS 18974 → starting from square one?
Increasing number of security incidents demands adequate OSS Management

Attacker with repository access pushed a malicious commit redirecting cryptocurrency to himself.

Many OSS users missed Log4J’s wake-up-call for OSS Security as still a significant share of the downloads of Log4J are vulnerable versions.

The attacker breached the build platform and embedded code that introduced harmful actions with every build.

Attacker added an innocent dependency and then later updated the dependency to add malicious behaviour.

"We don’t consider OSS to be less secure than Closed Source! Actually most Closed Source has OSS included anyway."

- Marcel Scholze, Head of OSS Services at PwC Germany
OSS Management is State of the Art
Governments and the private sector demand OSS security

"A SBOM describes the software components used as building blocks (...). These lists increase visibility into the product and enable (...) to check for known vulnerabilities and validate the device from a security standpoint, helping to reduce the vulnerability gaps (...)."

ENISA, Guidelines for Securing IoT (Nov. 2020)

"The digital operational resilience testing programme (...) shall provide (...) execution of appropriate tests, such as vulnerability assessments and scans, open source analyses (...) scanning software solutions, source code reviews where feasible (...)."

Digital Operational Resilience Act (Jan. 2023)

"Due to both the unique strengths of open source software and inconsistent historical investment in open source software security, there exist unique challenges in securing open source software (...) and the Federal Government should play a supporting role in ensuring the long-term security of open source software (...)."

Securing Open Source Software Act (Sept. 2022)

"Manufacturers shall, upon identifying a vulnerability in a component, including in an open source component, which is integrated in the product with digital elements, report the vulnerability to the person or entity maintaining the component. (...)"

Cyber Resilience Act (Draft, Sept. 2022)

More Security in Software Supply Chains is dependent on:
... more transparency in software use
... more standardization of OSS Management Practices
... more standardization of information bases

The new ISO 18974 – ISO 5230 as a stepping stone?
PwC
Introduction to ISO/IEC DIS 18974
What the new ISO for Open Source Security looks like

Background and focus

- Following OpenChain ISO 5230:2020
- Transfers ISO 5230 into the security domain
- Serves as the official guide for OSS Security Assurance programs
- Describes “what” and “why” aspects of Security Assurance, allowing for flexibility in implementation
ISO 18974 – Implementation Areas (1/2)
Requirements on Open Source Security for Supplied Software

Adherence to the Guidelines Requirements
- Completeness
- Conformance
- Duration

Open Source Content Review and Approval
- Software Bill of Materials (SBOM)
- Security Assurance

ISO 18974

Program Foundation
- Policy
- Competence
- Awareness
- Program Scope
- Standard Practice Implementation

Relevant Tasks Defined and Supported
- Access
- Effectively Resourced

The new ISO 18974 – ISO 5230 as a stepping stone?
ISO 18974—Implementation Areas (2/2)
Requirements on Open Source Security for Supplied Software

Adherence to the Guidelines Requirements
Excerpt of exemplary deliverables:
- documented evidence affirming the Program satisfies all the requirements
- ...

Open Source Content Review and Approval
Excerpt of exemplary deliverables:
- documented procedure for creating and maintaining SBOMs for Supplied Software
- documented procedure for handling detection and resolution of Known Vulnerabilities of the Supplied Software
- ...

Program Foundation
Excerpt of exemplary deliverables:
- written policy for OSS Security Assurance
- documented list of roles with corresponding responsibilities and competencies
- ...

Relevant Tasks Defined and Supported
Excerpt of exemplary deliverables:
- publicly visible method that allows any third party to make Known Vulnerability or Newly Discovered Vulnerability inquires
- identified Program roles have been properly staffed, adequate funding allocated
- ...

The new ISO 18974 – ISO 5230 as a stepping stone?
The core of ISO 18974 is supply chain security
Conformance builds trust in the supply chain
Synergies of strategic ISO implementation → ISO 5230 as a stepping stone for OSS security
Synergies of ISO 5230 and ISO/IEC DIS 18974
Comparison of compliance and security related requirements

ISO 5230 areas
- Policies on OSS License Compliance and Community Engagement
- Scope of OSS License Compliance Program
- Competencies
- Awareness

License Compliance Measures:
- Handling of OSS license use cases
- Compliance Artifact Creation and Delivery

ISO 18974 areas
- Policies on OSS Security
- Scope of OSS Security Program
- Competencies
- Awareness

Security Assurance Measures:
- Detection and resolution of Known Vulnerabilities
- Maintenance of records
- Information of clients of supplied SW

Program Foundation
Relevant Tasks Defined and Supported
SBOM
process for creating and maintaining a software bill of materials that includes each Open Source component from which the Supplied Software is comprised

The new ISO 18974 – ISO 5230 as a stepping stone?
ISO 5230 as a stepping stone towards OSS Security?
SBOMs are a crucial element in both ISO standards

• Both ISO standards require robust Program Foundation (Policies, Scoping, Awareness, Trainings)
• The introduction of ISO 5230 and 18974 should be oriented towards existing frameworks
• Procedures of SBOM Creation and Maintenance are a crucial element in both ISO standards and should be properly harmonized

Advantageous synergies during implementation can be realized regardless of the implementation scenario:
• one of the two ISO standards is already implemented
• implemented one after the other
• implementation in parallel
ISO 18974 as an important milestone to OSS Security

- Resilient IT systems require OSS security
- ISO 5230 can be a stepping stone
- Supply Chain security is a joint effort
- Contribution to OSS ecosystem
Please ask your questions or get in touch:

Katharina Grauf
OSS Expert
@ PwC Germany

+49 160 5526026

katharina.grauf@pwc.com

www.pwc.de/opensource

Enable digital future & Reduce risks

Consulting & Implementation  Audit & Certification  Managed Services

The new ISO 18974 – ISO 5230 as a stepping stone?