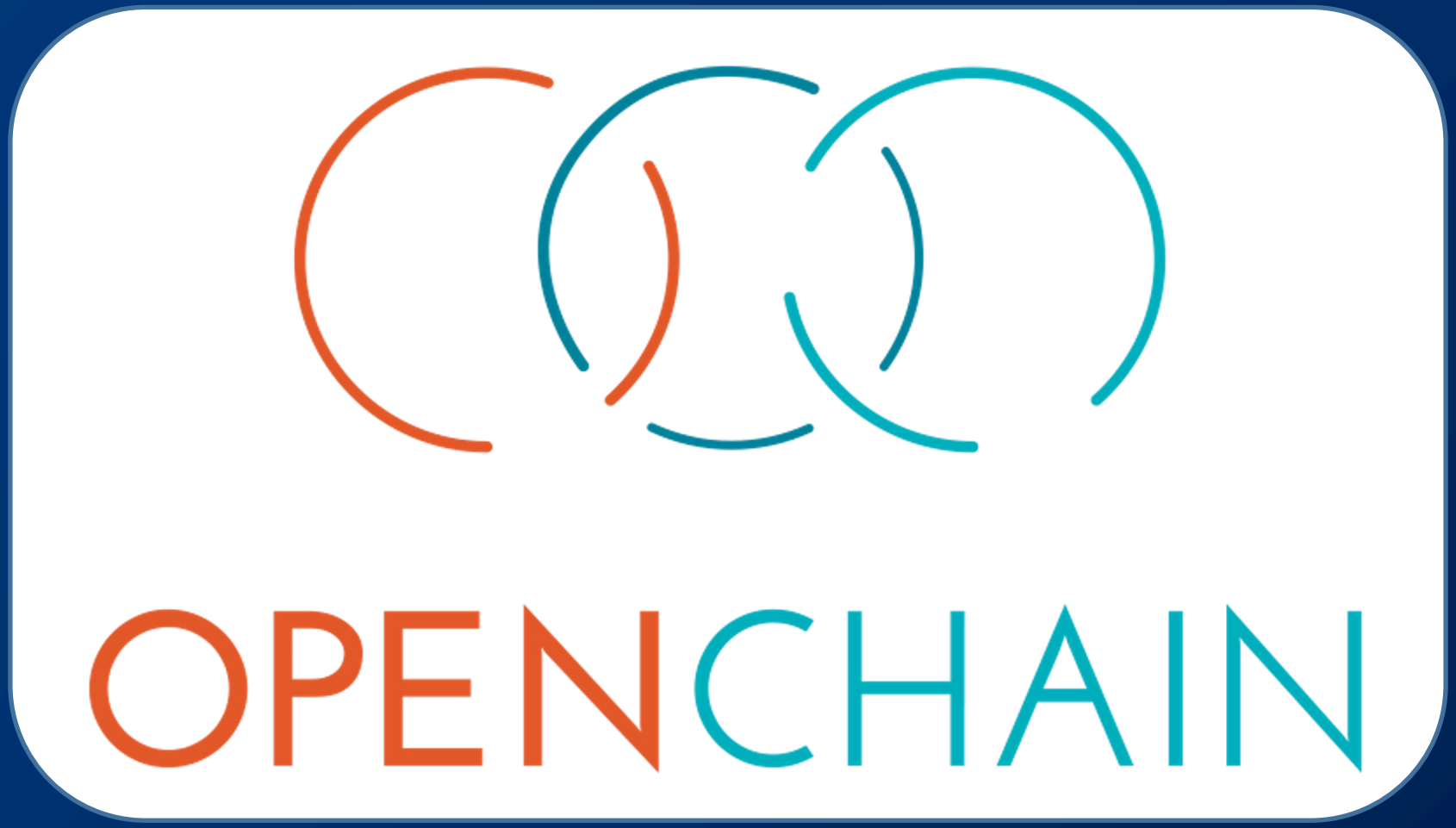


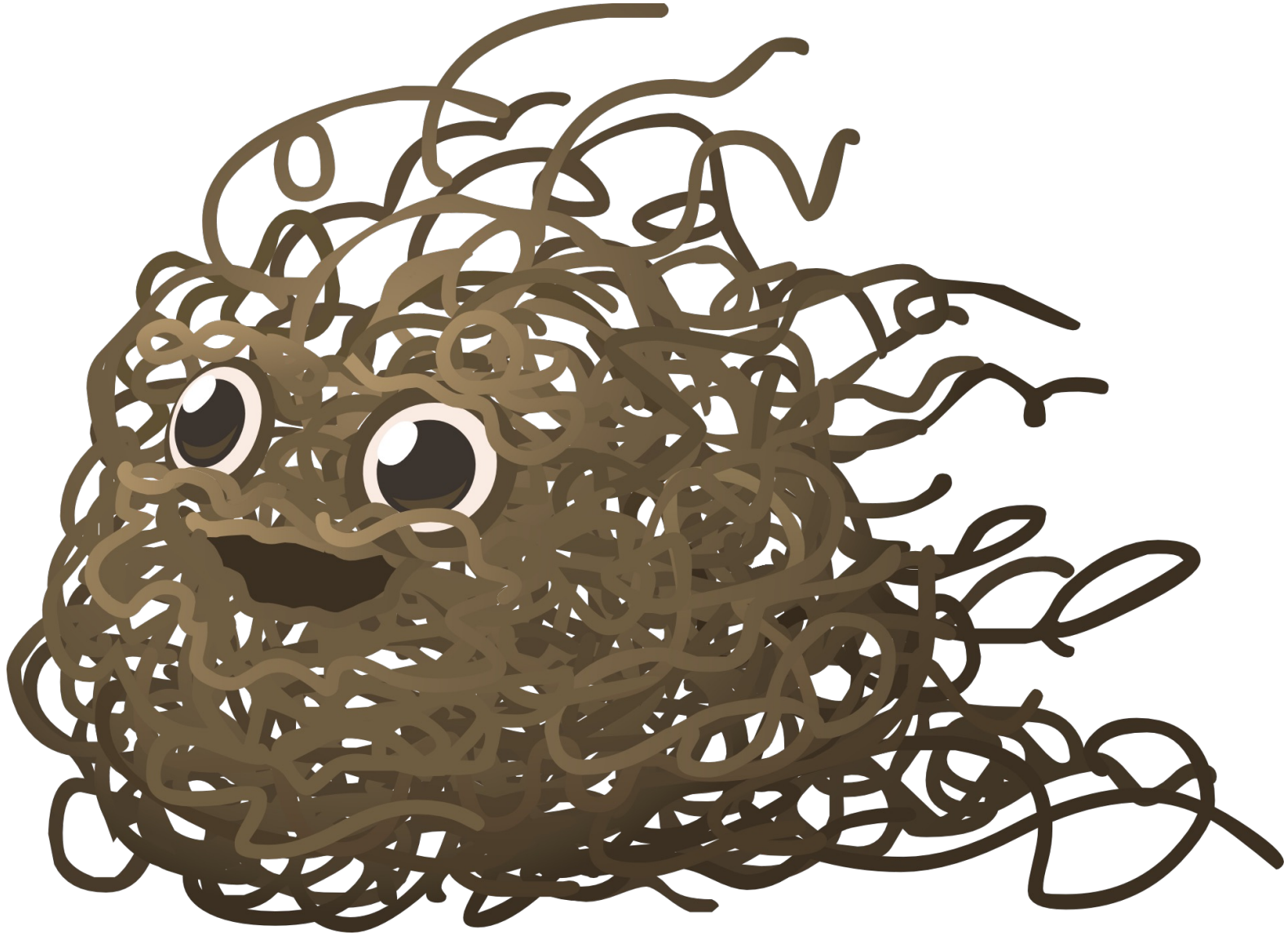
How The Linux Foundation Standards For License Compliance And Security Will Fix Your Supply Chain

Our Mental Model Of The Supply Chain

OPENCHAIN

The Actual Supply Chain

OPENCHAIN



OPENCHAIN

67.4%

of managers monitor their supply chain with Excel spreadsheets

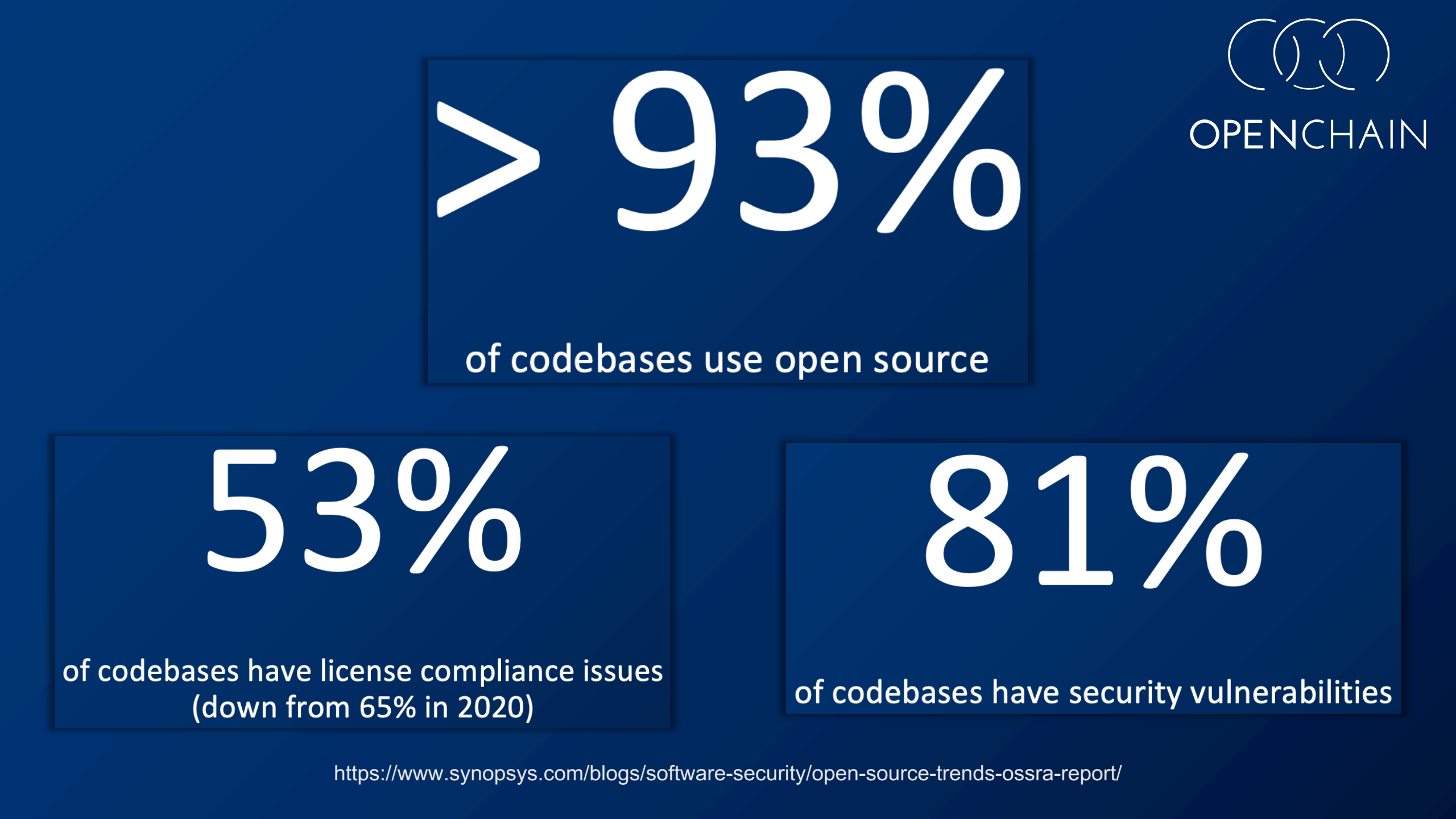
https://www.zippia.com/advice/supply-chain-statistics/

OPENCHAIN

94%

of companies do not have full visibility of their supply chain

https://www.zippia.com/advice/supply-chain-statistics/


OPENCHAIN
> 93%
of codebases use open source
53%
of codebases have license compliance issues
(down from 65% in 2020)
81%
of codebases have security vulnerabilities
https://www.synopsys.com/blogs/software-security/open-source-trends-ossra-report/

OPENCHAIN

40%

potential savings available via supply chain optimization

57%

of companies see supply chain management as a competitive edge

70%

of companies see supply chains as a driver for customer service

https://www.zippia.com/advice/supply-chain-statistics/

Context: This Is Important To Business

OPENCHAIN

Open Source License Compliance and Security Assurance
is a key part of supply chain management.

We Got Together To Improve The Supply Chain

OPENCHAIN

arm

BLOCK

BMW GROUP
BMW Car IT

BOSCH

CISCO

COMCAST

ERICSSON

FUJITSU

Google

HITACHI
Inspire the Next

HONOR

HUAWEI

Meta

Microsoft

MOXA

NEC

oppo

Panasonic

Qualcomm
Qualcomm Technologies, Inc.

SIEMENS

SONY

TOSHIBA

TOYOTA

Uber

Broader Community

OPENCHAIN

Main Work Groups:

- Specification (Spring 2016~)
- Education (Autumn 2020~)

Community Work Groups:

- Tooling (Summer 2019~)
- Export Control (Winter 2022~)
- Public Policy (Winter 2022~)

Special Interest Groups:

- Automotive (Summer 2019~)
- Telecom (Spring 2021~)

Regional User Groups

- Japan (Dec 2017~)
- Korea (Jan 2019~)
- India (Sept 2019~)
- China (Sept 2019~)
- Taiwan (Sept 2019~)
- Germany (Jan 2020~)
- UK (June 2020~)
- USA (Dec 2020~)

OPENCHAIN

1,000+

Companies Working On A Better Supply Chain

Trust Built By Process Management

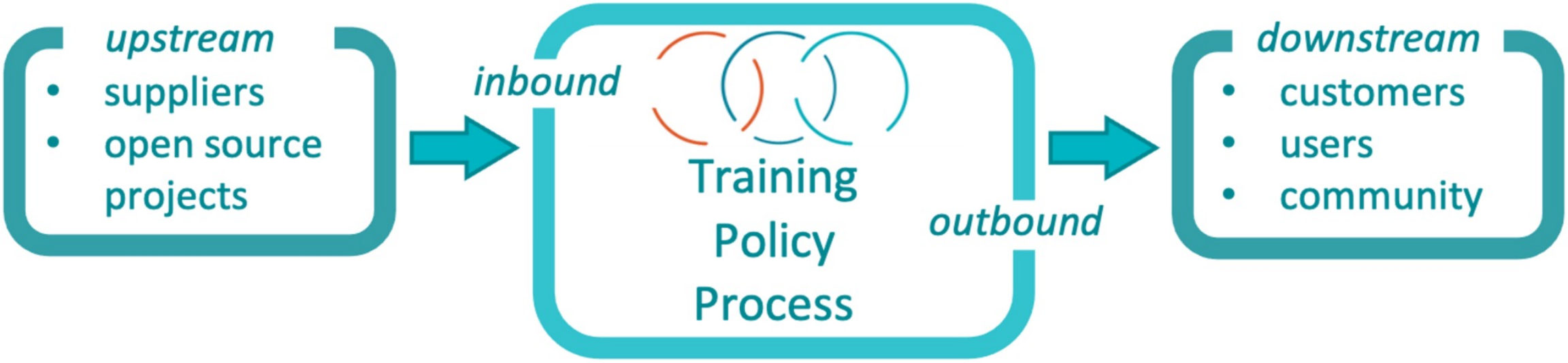
- **In Market Q4 2016~ (de facto) Q4 2020 (ISO/IEC)**
  OpenChain ISO/IEC 5230:2020
  The International Standard for open source license compliance.

- **In Market Q4 2022~ (de facto) Q3 2023 projected (ISO/IEC)**
  ISO/IEC DIS 18974, OpenChain Security Assurance Specification
  The de facto standard for open source security assurance compliance.

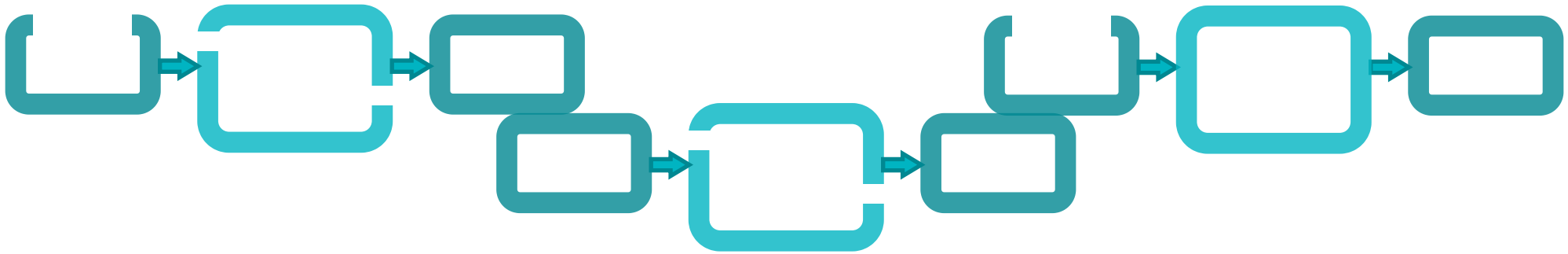
1. High level process standards;
2. Simple, effective and suitable for companies of all sizes in all markets;
3. Openly developed by a vibrant user community and freely available to all.

The Standards Work Company By Company

OPENCHAIN



Result = A More Predictable Supply Chain



Example Adoption Of OpenChain ISO/IEC 5230:2020

OPENCHAIN

20%

of German companies with over 2,000 employees
already use OpenChain ISO/IEC 5230

https://www.pwc.de/en/digitale-transformation/pwc-bitkom-study-open-source-monitor-2021.pdf

Security Assurance Specification Traction

BlackBerry Announces First North American OpenChain Security Assurance Specification Conformance

By Shane Coughlan | 2023-01-24 | Featured, News

BlackBerry Limited (NYSE: BB; TSX: BB) announces adoption of the OpenChain Security Assurance Specification 1.1, creating a series of landmarks in doing so. BlackBerry is the first whole entity to announce conformance, the first conformance in the Americas, the first multinational company conformance, and first entity to achieve conformance with both OpenChain/ISO5230:2020 and OpenChain Security Assurance 1.1 with an OpenChain Partner, OSS Consultants. This announcement builds on their previous adoption of OpenChain ISO/IEC 5230:2020, the international standard for open source license compliance. OpenChain Security Assurance Specification 1.1 is the sister standard to ISO/IEC 5230, and is also slated to become an ISO standard later in 2023.

Freedom Of Choice In Using Our Standards

OPENCHAIN

1. Self-Certification
2. Independent Assessment
3. Third-Party Certification

Free Self-Certification Material

OPENCHAIN

Section 1: Program foundation

- [ ] We have a policy governing the open source license compliance of Supplied Software.
- [ ] We have a documented procedure to communicate the existence of the open source policy to all Software Staff.
- [ ] We have identified the roles and responsibilities that affect the performance and effectiveness of the Program.
- [ ] We have identified and documented the competencies required for each role.
- [ ] We have documented the assessed competence for each Program participant.
- [ ] We have documented the awareness of our Program participants on the following topics:
  - [ ] The open source policy and where to find it;
  - [ ] Relevant open source objectives;
  - [ ] Contributions expected to ensure the effectiveness of the Program;
  - [ ] The implications of failing to follow the Program requirements.
- [ ] We have a process for determining the scope of our Program.
- [ ] We have a written statement clearly defining the scope and limits of the Program.
- [ ] We have a documented procedure to review and document open source license obligations, restrictions and rights.

Section 2: Relevant tasks defined and supported

- [ ] We assigned individual(s) responsibility for receiving external open source compliance inquiries.
- [ ] The external open source compliance contact is publicly identified (e.g. via an email address or the Linux Foundation Open Compliance Directory).
- [ ] We have a documented procedure for receiving and responding to open source compliance inquiries.
- [ ] We have documented the persons, group or function supporting the Program role(s) identified.
- [ ] We have ensured identified Program roles been properly staffed and adequately funded.
- [ ] Legal expertise to address internal and external open source compliance has been identified.
- [ ] We have a documented procedure assigning internal responsibilities for open source compliance.

11 Third-Party Certifiers Providing Global Coverage

OPENCHAIN

BUREAU VERITAS

CAICT 中国信通院

中国电子技术标准化研究院 China Electronics Standardization Institute

ISCAS

ORCRO

OSPOCO

pwc

SYNOPSYS®

TIMETOACT SOFTWARE & CONSULTING

TÜVNORD

TÜV SÜD

Free Online Training Courses

OPENCHAIN

Introduction to Open Source License Compliance Management (LFC193)

Implementing Open Source License Compliance Management (LFC194)

1. LFC193 - 1209 total enrollments (398 digital badges issued)
   4.65 out of 5 rating by users
2. LFC194 - 579 total enrollments (138 digital badges issued)
   4.55 out of 5 rating by users

Example Of Market Use

OPENCHAIN

Continental ♥ Introduction to Open Source License Compliance Management (LFC193)

Continental made LFC193 a required course for their software developers from late Q3

BOSCH ♥ Introduction to Open Source License Compliance Management (LFC193)

Bosch has asked suppliers and requires external developers to use LFC193 since Q4 2021

KPMG ♥ Introduction to Open Source License Compliance Management (LFC193)

KPMG AG asks their developers and architects to complete LFC193

Continually Expanding Support Coverage

OPENCHAIN

OpenChain Security Assurance Specification 1.1 – Global Support

By Shane Coughlan | 2022-12-14 | Featured, News

BUREAU VERITAS · CAICT 中国信通院 · ORCRO · OSS CONSULTANTS · pwc · Source Code Control Open Source Risk Management Specialists

The OpenChain Security Assurance Specification 1.1 has been building momentum as a sister specification to ISO/IEC 5230:2020, the International Standard for open source license compliance. With an identical approach to high level process management, the OpenChain Security Assurance Specification is designed to help companies adopt the key requirements of a quality open source security assurance program.

Bitsea Announces OpenChain Security Assurance Services

2023-01-12

OSPOCO and Taylor English Join The OpenChain Partner Program

2023-02-07

TIMETOACT GROUP Offers Open Source Certification Based On ISO/IEC 5230

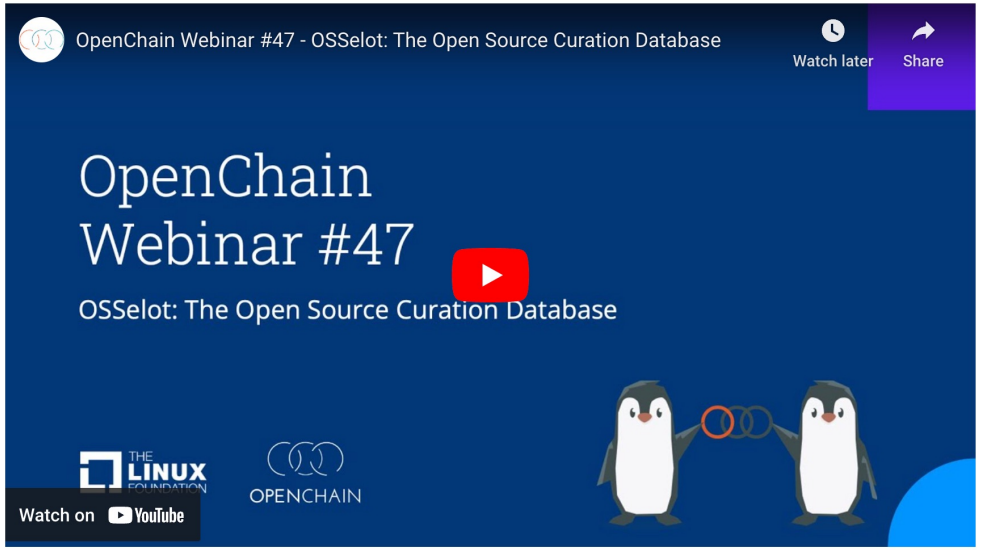
2023-02-08

Continually Expanding Industry Knowledge

OpenChain Webinar #47 – OSSelot: The Open Source Curation Database

By Shane Coughlan | 2023-01-25 | Featured, News, Webinar

This OpenChain Webinar features OSSelot, an open source curation database recently launched by OSADL in Germany. This project addresses one of the most requested features around open source automation for open source compliance: an open, public database supporting SBOM (via SPDX ISO/IEC 5962) for common software packages. This could be a game-changer.



OpenChain Webinar #48 – GPLv2 Licensing History

By Shane Coughlan | 2023-02-15 | Featured, News, Webinar

This OpenChain Webinar features an overview of GPLv2 licensing fragmentation based on research initiated by Philippe Ombredanne of NexB and continued by Armijn Hemel of Tjaldur Software Governance Solutions. The key takeaway is that a significant number of variations exist (40 “vanilla” copies from the FSF or GNU website, 12 with the Linux kernel linking exception in the Linux kernel), but the impact of these variations is nuanced. The requirements do not change but the variability may throw errors for automation and review. Process awareness is required.

Actively Editing The Next Generation Standards

OPENCHAIN

OpenChain Monthly Meeting North America – Europe – 2023-02-07 – Recording

By Shane Coughlan | 2023-02-10 | Featured, News

We had a fantastic meeting focused on editing previously submitted scope suggestions from ISO/IEC WG/SC 27 (Information Technology Security). This time we went over issues submitted by reviewer CERT. In addition to this, we closed an open issue syncing the definition of Open Source between the licensing (ISO 5230) and security specifications.

Co-chairs Helio and Chris lead the discussion, and we had some great contributions from the audience. It is clear that there is significant interest in reviewing the draft 3rd generation licensing standard and 2nd generation security standard. You are reminded that everyone is invited to participate on the monthly calls and via our main or specification mailing lists.

Specifically..

We closed this open source definition issue:
https://github.com/OpenChain-Project/Security-Assurance-Specification/issues/20

We set this action item based on a suggestion by CERT:
https://github.com/OpenChain-Project/Security-Assurance-Specification/issues/22

We decided not to pursue this suggestion by CERT:
https://github.com/OpenChain-Project/Security-Assurance-Specification/issues/23

We decided not to pursue this suggestion by CERT:
https://github.com/OpenChain-Project/Security-Assurance-Specification/issues/24

Be Part Of This

OPENCHAIN

https://www.openchainproject.org/participate