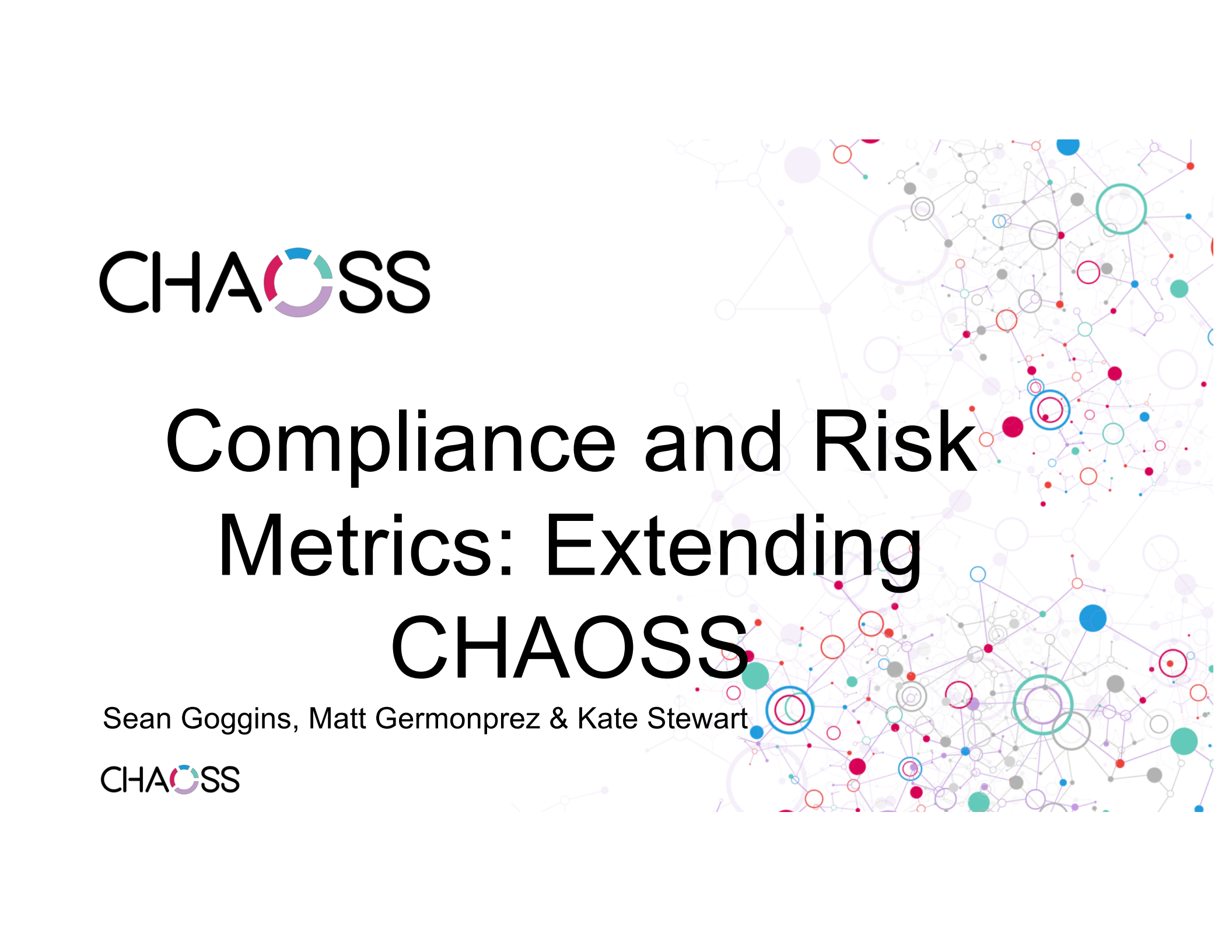


Compliance and Risk Metrics: Extending CHAOSS

Sean Goggins, Matt Germonprez & Kate Stewart

CHAOSS

Working in an Open Community...

eclipse

openstack™

SYMPHONY SOFTWARE FOUNDATION

Software Sustainability Institute

Bitergia

mozilla

redhat.

CLOUD NATIVE COMPUTING FOUNDATION

Linaro

SAUCELABS

SECO Health

THE LINUX FOUNDATION

University of Nebraska Omaha

University of Missouri

University of Victoria

JONO BACON CONSULTING

CHAOSS

CHAOSS Mission

Establish implementation-agnostic metrics for measuring community activity, contributions, and health.

Produce integrated, open source software for analyzing software development in terms of these metrics.

CHAOSS

Metrics Committee

Diversity-Inclusion	Growth-Maturity-Decline
Risk	*Value*

wiki.linuxfoundation.org/chaoss/metrics

CHAOSS

Diversity and Inclusion are known to challenge unchecked assumptions and lead to more open and fair collaboration practices.

An OSS community has states: ***Growth, Maturity, and Decline***. The state that a community is in may prove important when evaluating both across and within community concerns.

The ***Risk*** metric informs how much risk an OSS community might pose. The evaluation of risk depends on situation and purpose.

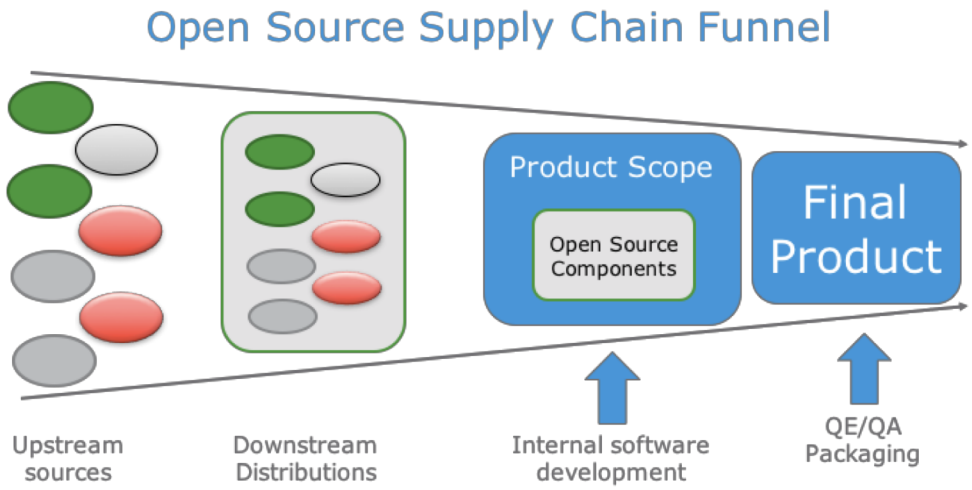
Developers and organizations capture ***Value*** from engaging in OSS communities. This set of metrics can inform what this value is.

CHAOSS

Cases: Procurement Supply Chain

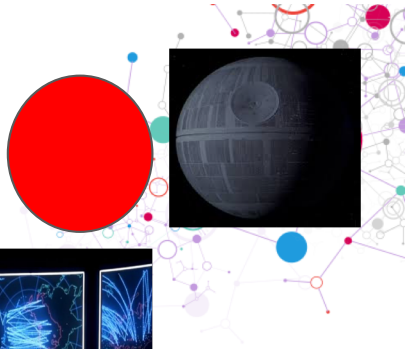
Metrics Stakeholders

1. Developer Metrics
2. Contract Lawyer Metrics
   a. Licensing
   b. Software Bill of Materials
3. Consumers of software products, Especially Safety Critical
   a. Badging to show that some kind of enterprise best practices are followed.
   b. Accountability at the other end of the supply chain
   c. Software bill of materials



opensource.com

CHAOSS Mission



Risk:

1. Likelihood of loss
2. Impact of loss

Impact of Loss

Likelihood of Loss

CHAOSS

Software Considerations in a Trustworthy Device

Trustworthy Device –a medical device containing hardware, software, and/or programmable logic that:

(1) is reasonably secure from cyber security intrusion and misuse;

(2) provides a reasonable level of availability, reliability, and correct operation;

(3) is reasonably suited toperforming its intended functions; and (4) adheres to generally accepted security procedures.

What is Reasonably secure?

CHAOSS

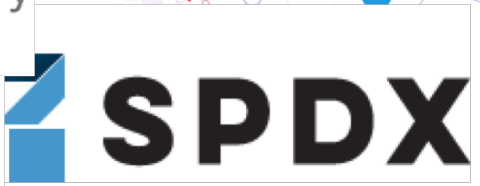
fossbytes.com

Risk Questions: Risks to using software

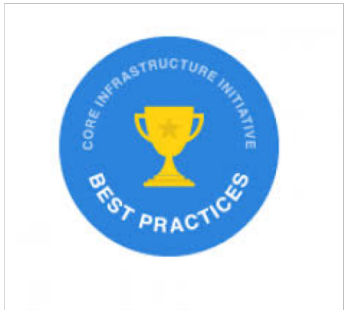
1. What is the quality of your code?
2. Are you allowed to use it?
3. When you use it is it safe?
4. Can you be subverted in the future?

CHAOSS

Projects



1. SPDX, FOSSology, DOSoCS
2. Zephyr: Safety and Security
3. ELISA: Enabling linux in safety critical applications
4. CII: Security best practices
    a. Extend or expand into quality and licensing?
    b. Ecosystem needs to support more than security
    c. Quality

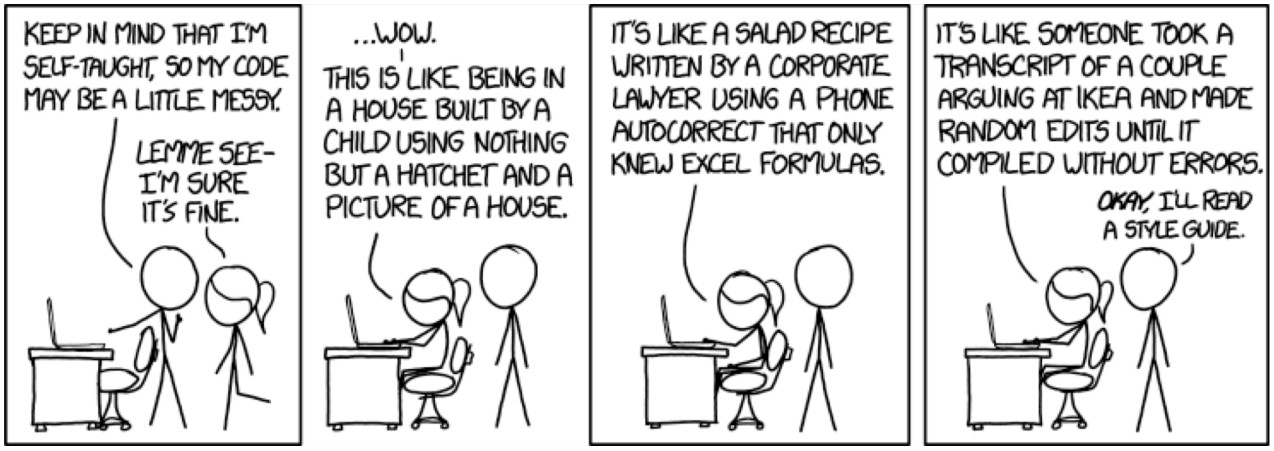


CHAOSS

Five Domains of Risk

1. Accurate Identification
2. Code Quality
3. Cybersecurity
4. Safety critical use
5. Licensing

xkcd



CHAOSS

Risk Metrics: Next Steps

1. Who is interested in working in these domains?
2. Which domains?
3. What are some metrics you would like to see in the domains that are interesting and important to you?
4. Are there areas of risk that are important to consider that are not listed here?

CHAOSS

Online Live Survey

Added later.

CHAOSS

Thank You

CHAOSS