

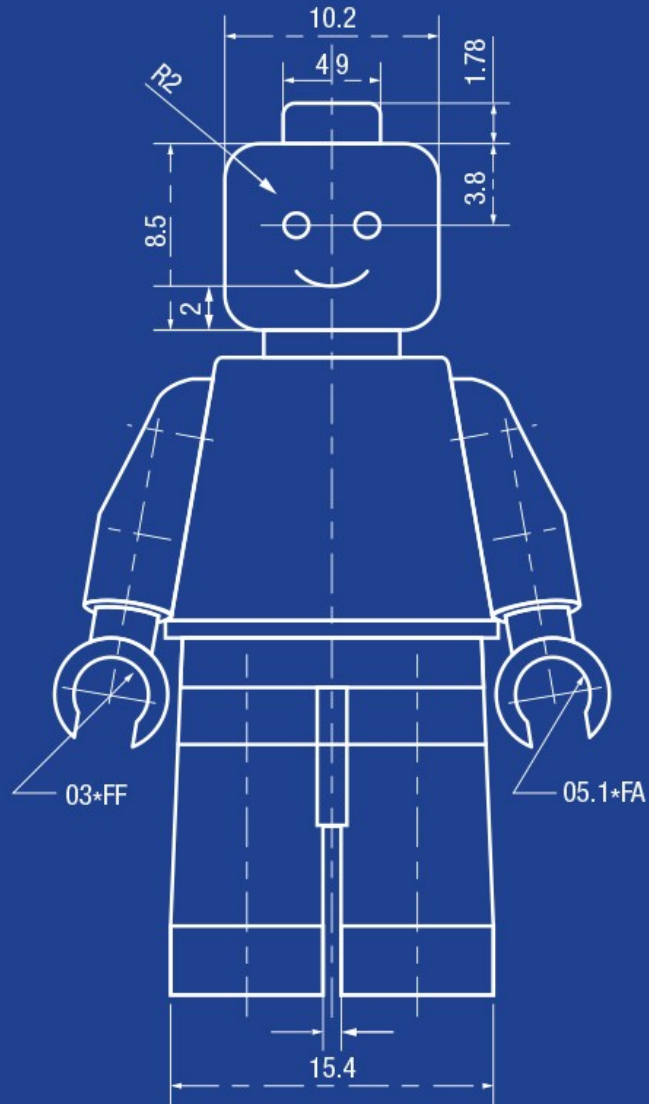


LUND
UNIVERSITY

Health and Sustainability of Open Source Software from a Public Sector Perspective

JOHAN LINÅKER, PHD





About Johan



Open Source Software Sustainability

- An Open Source Software project's capability to stay maintained at length without interruption or weakening



Open Source Software Health

- An Open Source Software project's ability to stay viable over time
 - Productivity: There is an active development of the project
 - Robustness: The development is open and spread out on several (independent) individuals
 - Openness: Users of the project can influence and contribute to the development of the project

The background of the slide is a photograph of the Golden Gate Bridge in San Francisco. The bridge's towers and suspension cables are visible against a blue sky with light clouds. The bridge deck is filled with cars, and the water of the bay is visible below. A semi-transparent white box is overlaid on the left side of the image, containing the title text.

Open Source Software and our Digital Infrastructure

- Open Source Software makes up a vitale building block in our digital infrastructure
- Needs maintenance as with physical infrastructure to stay secure and robust



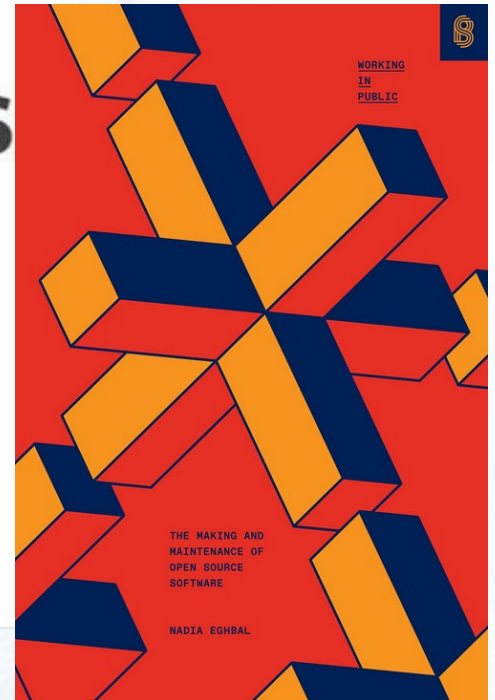
Open Source Software and our Digital Infrastructure

- Recommended reading by Nadia Eghbal
 - Roads and Bridges
 - Working in Public: The Making and Maintenance of Open Source Software

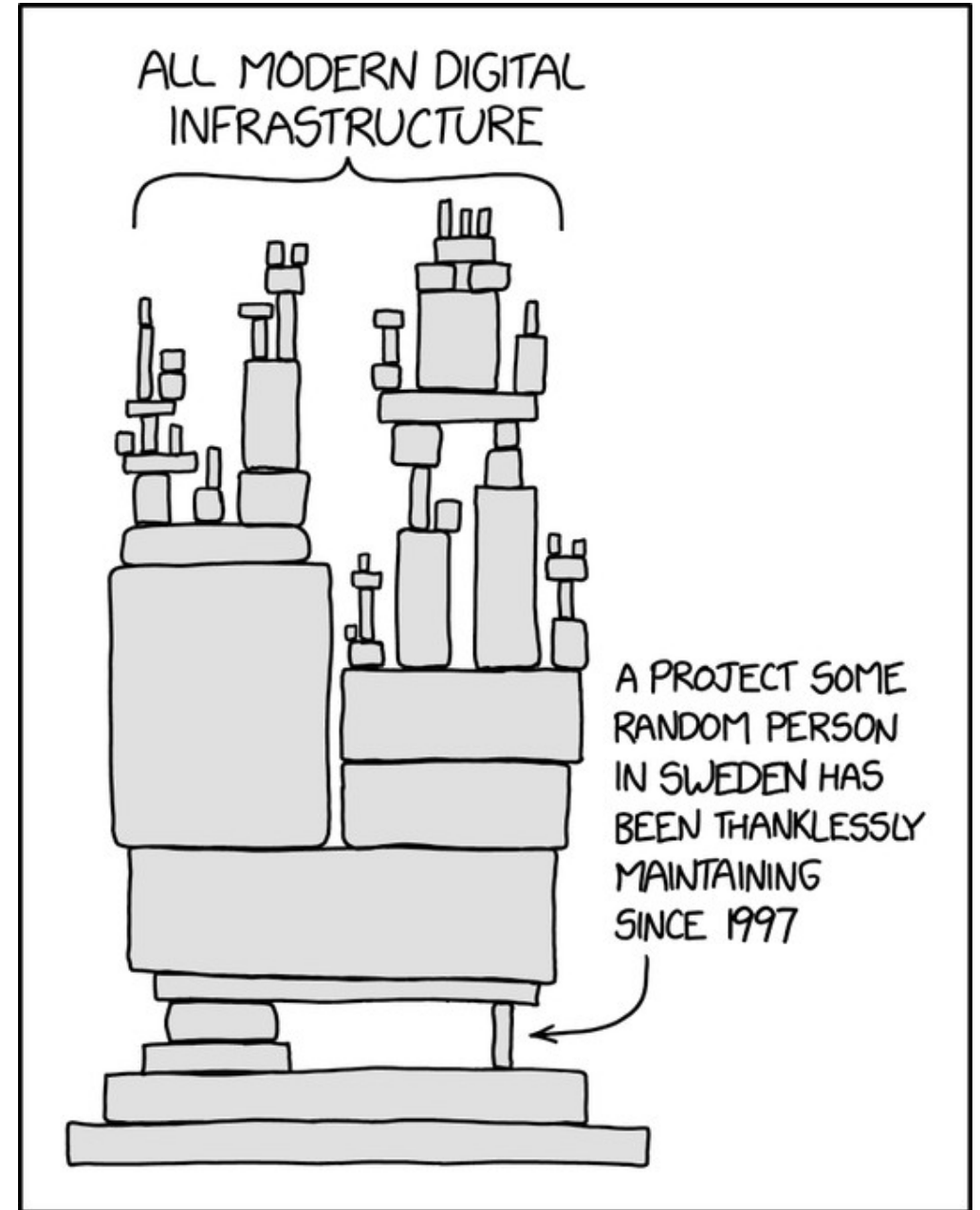


Roads and Bridges

The Unseen Labor Behind
Our Digital Infrastructure



Open Source Software and our Digital Infrastructure





The Dualism of Quality

- Open Source Software is...
 - full of, or receptive to, vulnerabilities ready to be exploited
 - always more secure than proprietary alternatives

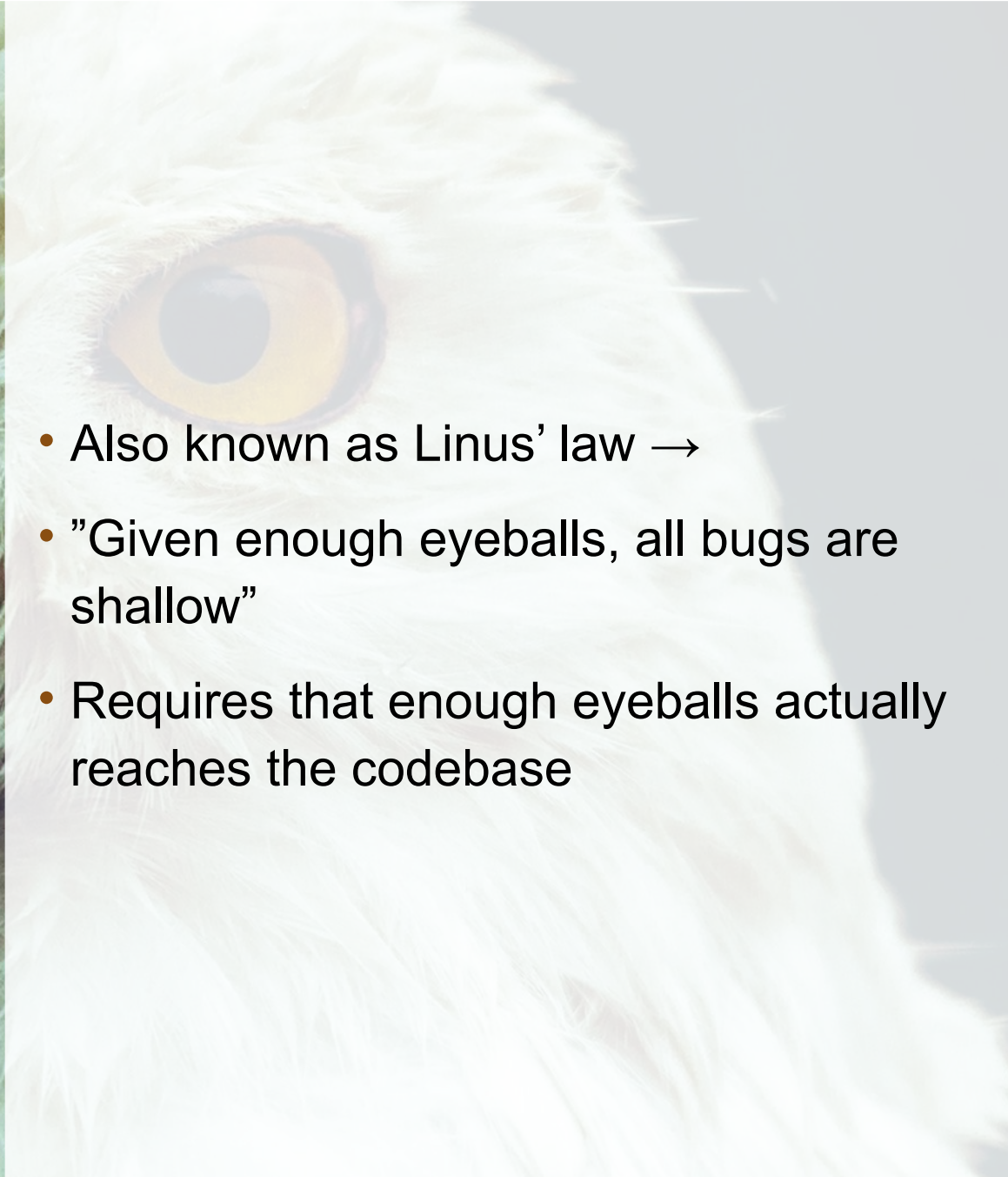
Example: Heartbleed

- A bug introduced into the OpenSSL cryptography library
- Used in a large part of the world's connected devices
- Introduced in 2012, fixed in 2014
- Enabled access to private identification keys
- Was maintained by two individuals at time of introduction while used by (almost) everyone



The "Many-Eyes" effect



- 
- Also known as Linus' law →
 - "Given enough eyeballs, all bugs are shallow"
 - Requires that enough eyeballs actually reaches the codebase



Development Resources are Depletable

- Maintainers are humans, not robots
 - Burnout, changed family or working conditions
- Companies must adapt to stay competitive
 - Refactorization, new products, changed business model




Who's responsible for ensuring the SW quality?



- Maintainer(s)?
- Developer community?
- User community?
- Individuals vs. Companies vs. Government?



Open Source Software in the Public Sector

- 
- Challenged by lack of culture, knowledge and resources
 - Acquisition and public procurement key to adoption and development of open source software
 - Need for support and direction




The OSPO-approach: Example from Italy

- National and regional competence centers → Government Open Source Program Offices
- Law requiring use and release of Open Source Software
- Decision model and guidelines for how to evaluate and compare open source software, including:
 - *“the viability of the open source project, through the assessment of visible indicators on the repository, such as code activity, release history, user community, longevity of the project, number of unique developers.”*
- See: <https://docs.italia.it/italia/developers-italia/gl-acquisition-and-reuse-software-for-pa-docs/en/stabile/index.html>



The Foundation-approach: Example from Denmark

- OS2 – formal collaboration between majority of Danish municipalities → Government foundation
- Projects initiated by one or multiple municipalities, developed through procurement
- Ecosystem of 60+ vendors and service suppliers
- Established governance and collaboration models for new open source software projects
- See: <https://os2.eu/>



The Network-approach: Example from Sweden

- Network for Open Source and Data
- Network for public entities sharing knowledge and growing culture on the use and collaboration of open source software and open data
- Monthly workshops with 80-120 participants with diverse representation
- Software catalogue of open source software used by Swedish public entities
- Do what we can with available time and resources
- See: <https://nosad.se>




Health Assessment in Acquisition process

- Is the project secure, i.e., viable long-term?
- Enable comparance between open and closed alternatives



Health Assessment of Dependent Projects

- Identify projects in need of support where health is low or at risk
- Proactive risk management and security work
- (or just being a good open source citizen)



Need for general tools and process support

- ***...criteria that can be used to evaluate software security, include criteria to evaluate the security practices of the developers and suppliers themselves...***
- <https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/>

CHAOSS – a metric toolbox

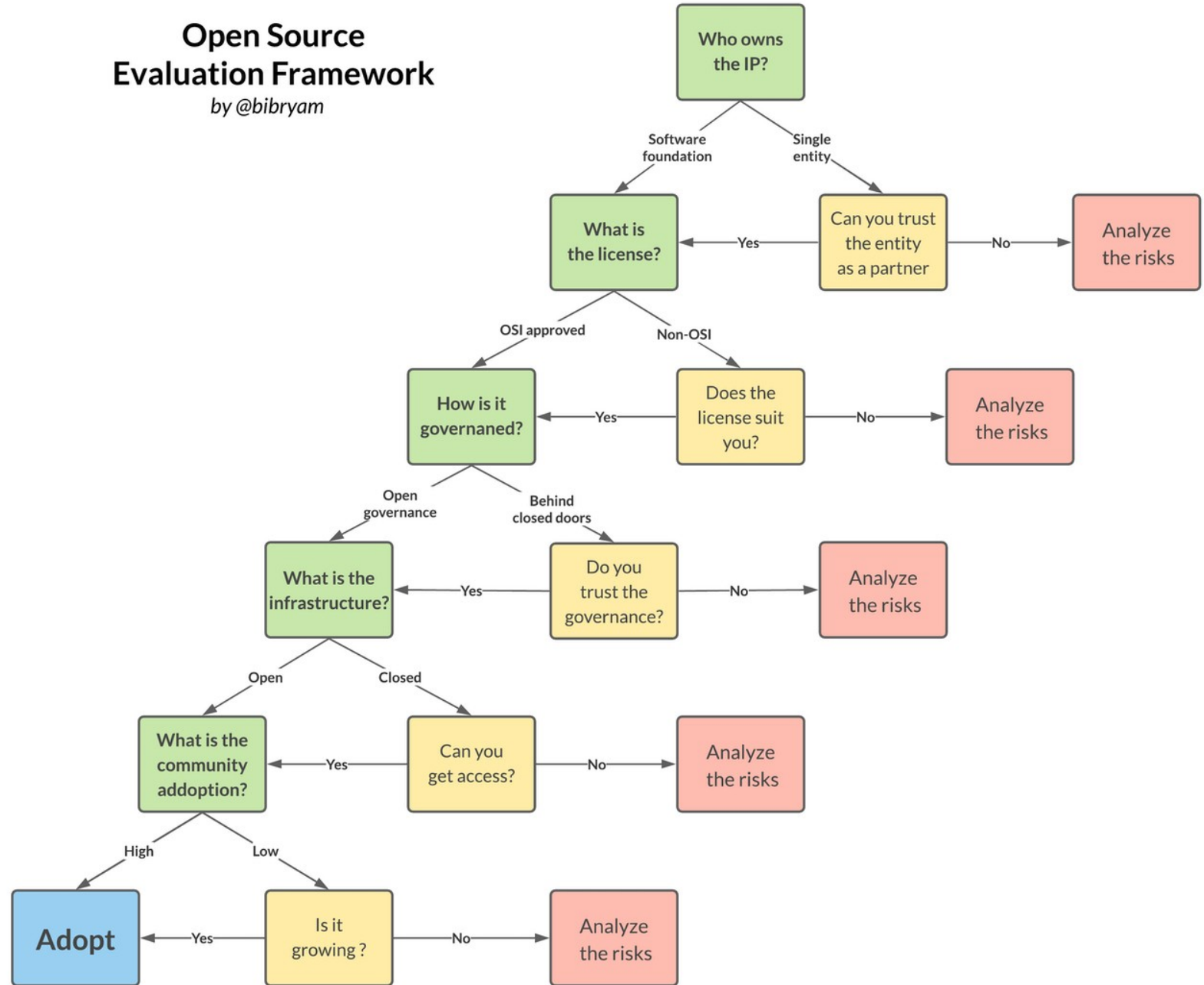
- Community Health Analytics for Open Source Software (CHAOSS)
 - Framework with metrics for health analysis and assessments
 - Five focus areas
 - Value
 - Risk
 - Evolution
 - Diversity and Inclusion
 - Common
- See: <https://chaoss.community>



Need for systemization



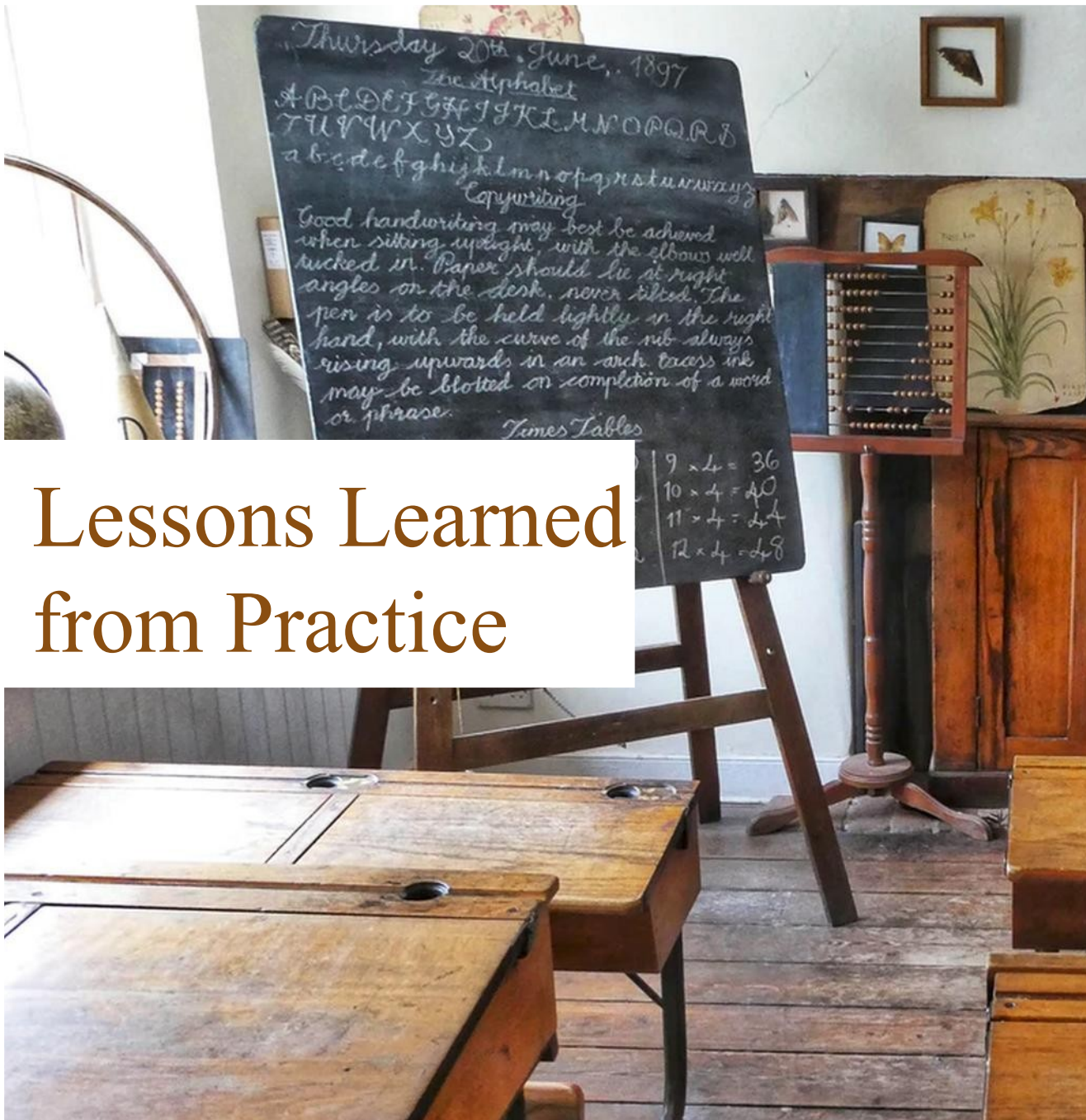
Open Source Evaluation Framework by @bibryam





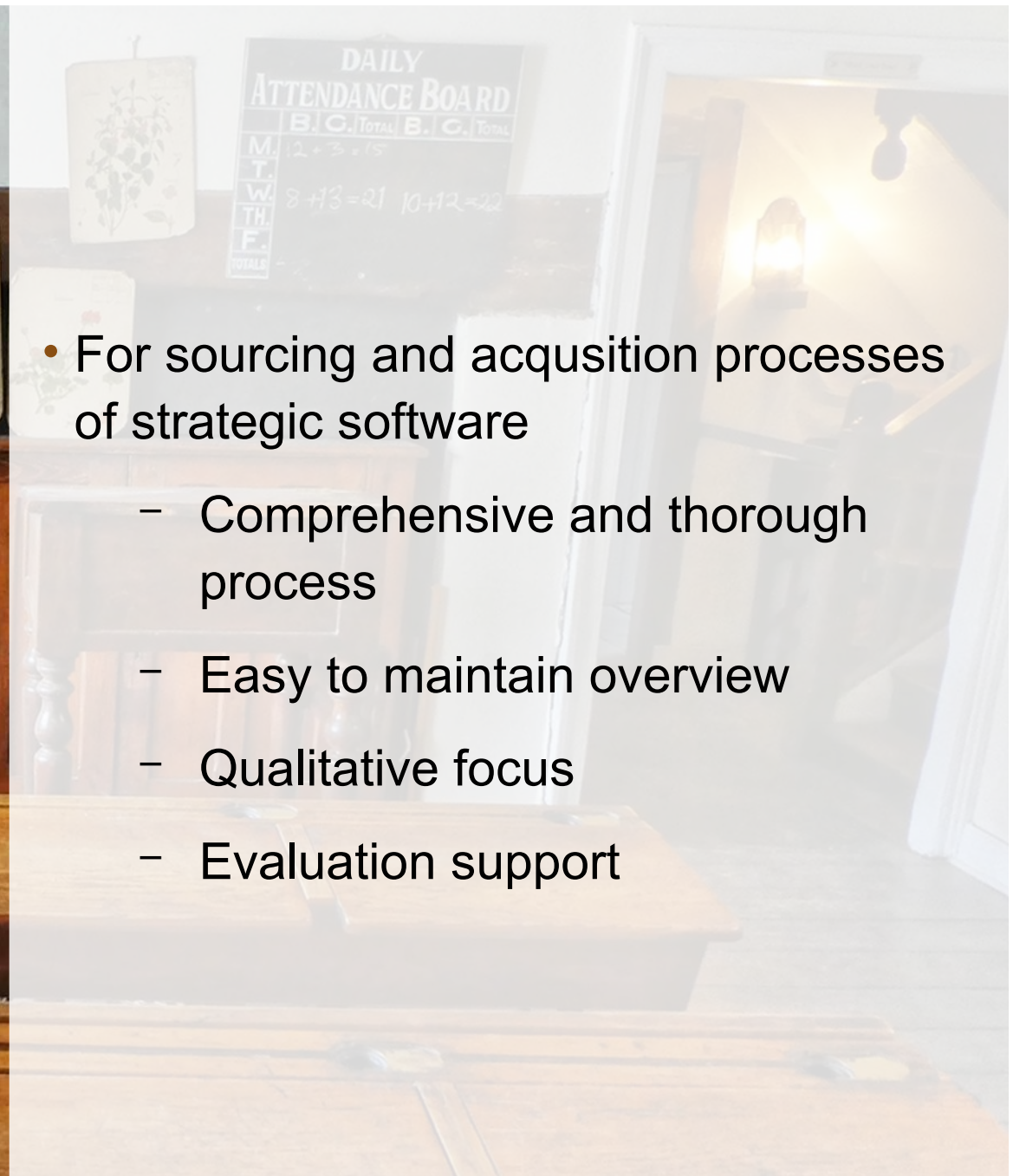
A qualitative approach to health assessment

- Legal – Ownership of copyright, type of license
- Governance – Openness for influence and appointment
- Accessibility – Communication and development
- Diversity – Users and developers
- Professionell support – Variety and types of services
- Social activity – Communication and development
- Development activity – Technical and non-technical
- Quality – Testcases, documentation, process etc.
- *Based on <https://CHAOSS.community> and <https://www.redhat.com/en/resources/open-source-project-health-checklist>*



Lessons Learned from Practice

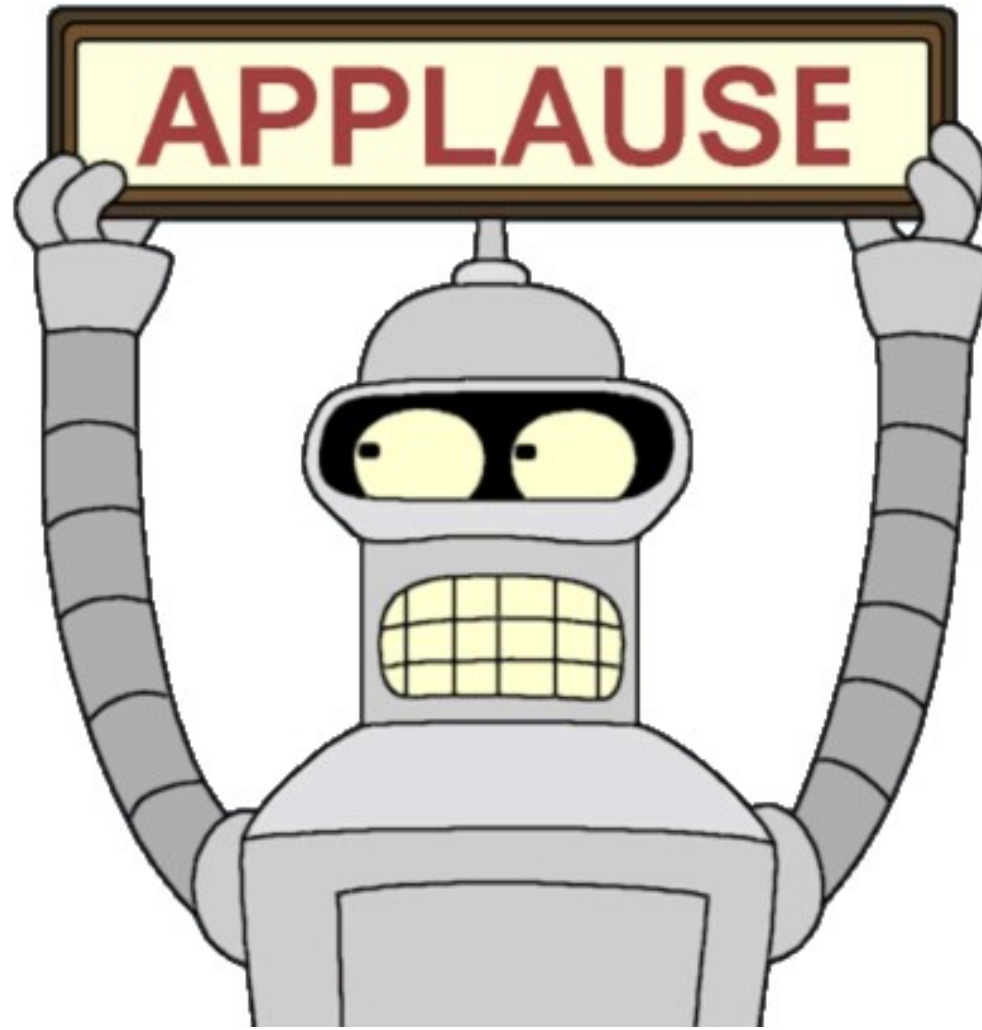
- For sourcing and acquisition processes of strategic software
 - Comprehensive and thorough process
 - Easy to maintain overview
 - Qualitative focus
 - Evaluation support





Final takeaways

- Health and sustainability of open source software is key to a secure and robust digital infrastructure
- Public sector (and everyone else) should consider what responsibility they have in terms of contributing to health of central open source software projects
- Public entities need support and direction in how they can use and develop open source software
- Health assessment should be integrated as a key practice in public acquisition processes





LUND
UNIVERSITY