Moving Beyond Compliance

Using a capability model to grow community excellence.
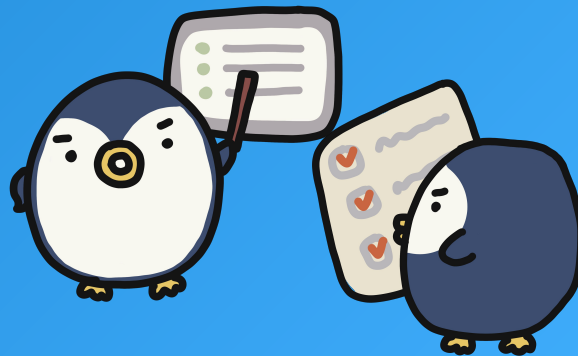
THE LINUX FOUNDATION

OPENCHAIN

Andrew Katz
CEO - Orcro Limited
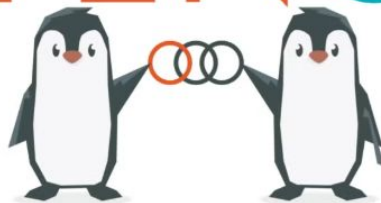
andrew.katz@orcro.co.uk

Stephen Pollard
Director - Orcro Limited

stephen.pollard@orcro.co.uk

Moving Beyond Compliance

- Introduction to Open Chain and the Education Working Group
- Why OpenChain is working on capability assessment methodologies
- Features of the model and tool
- Where to find the tool
- Opportunities for future collaboration

OOOPENCHAIN

BUILDING TRUST IN THE SUPPLY CHAIN SINCE 2016

Our vision is a supply chain where open source is delivered with trusted and consistent process management information. Our mission is to make that happen.

The OpenChain Project has an **extensive global community** of over 1,000 companies collaborating to make the supply chain quicker, more effective and more efficient. We work with our sister projects at The Linux Foundation like SPDX (SBOM), OpenSSF (Security), TODO Group (OSPO) and CHAOSS (Metrics) to help drive forward business management of open source.

We Maintain Standards

- **OpenChain ISO/IEC 5230**
  The international standard for open source license compliance programs
- **OpenChain ISO/IEC 18974**
  The industry standard for open source security assurance programs

Work of the OpenChain Education Workgroup

- Creating materials required for compliance with the standards
  - The OpenChain Curriculum
- Creating materials to help explain and promote openchain
  - Explainers
  - Videos
  - Supplier education leaflets
- Creating materials to assist organisations to implement and improve their OpenChain programs
  - Capability model
- Regular meetings: see https://openchainproject.org/participate

Why Use Capability Assessment Methods?

Compare / share best practice

Focus on operational excellence
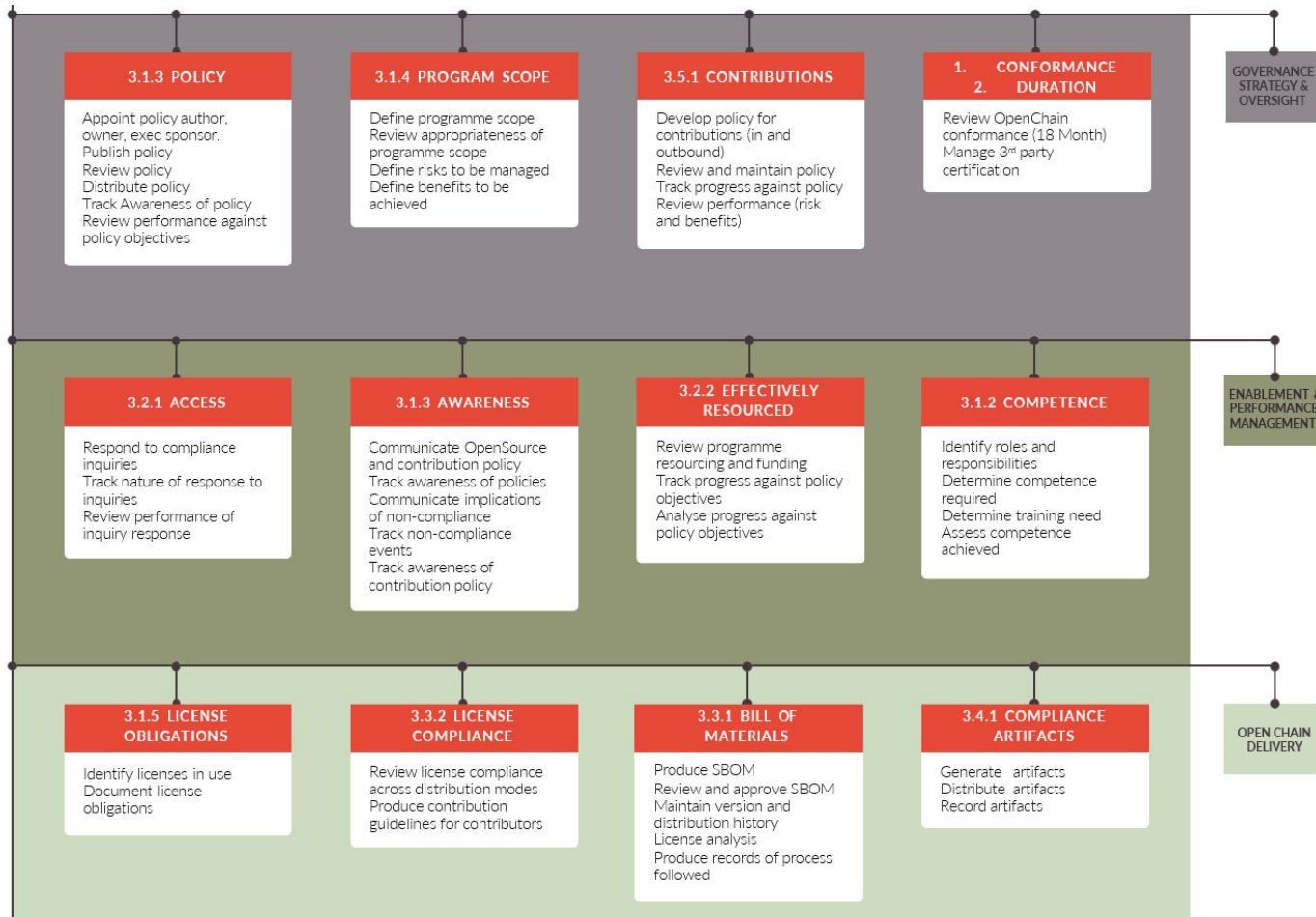
Build a business case for investment

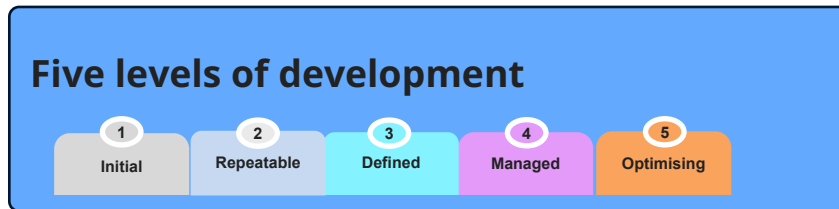Raise performance in different teams across a community

Handle new technologies or emerging risks (e.g. AI governance)

Funding rounds, M&A, Major Customer W&I

THE LINUX FOUNDATION

OPENCHAIN

ORCRO

GOVERNANCE STRATEGY & OVERSIGHT

3.1.3 POLICY

Appoint policy author, owner, exec sponsor.
Publish policy
Review policy
Distribute policy
Track Awareness of policy
Review performance against policy objectives

3.1.4 PROGRAM SCOPE

Define programme scope
Review appropriateness of programme scope
Define risks to be managed
Define benefits to be achieved

3.5.1 CONTRIBUTIONS

Develop policy for contributions (in and outbound)
Review and maintain policy
Track progress against policy
Review performance (risk and benefits)

1. CONFORMANCE
2. DURATION

Review OpenChain conformance (18 Month)
Manage 3rd party certification

ENABLEMENT & PERFORMANCE MANAGEMENT

3.2.1 ACCESS

Respond to compliance inquiries
Track nature of response to inquiries
Review performance of inquiry response

3.1.3 AWARENESS

Communicate OpenSource and contribution policy
Track awareness of policies
Communicate implications of non-compliance
Track non-compliance events
Track awareness of contribution policy

3.2.2 EFFECTIVELY RESOURCED

Review programme resourcing and funding
Track progress against policy objectives
Analyse progress against policy objectives

3.1.2 COMPETENCE

Identify roles and responsibilities
Determine competence required
Determine training need
Assess competence achieved

OPEN CHAIN DELIVERY

3.1.5 LICENSE OBLIGATIONS

Identify licenses in use
Document license obligations

3.3.2 LICENSE COMPLIANCE

Review license compliance across distribution modes
Produce contribution guidelines for contributors

3.3.1 BILL OF MATERIALS

Produce SBOM
Review and approve SBOM
Maintain version and distribution history
License analysis
Produce records of process followed

3.4.1 COMPLIANCE ARTIFACTS

Generate artifacts
Distribute artifacts
Record artifacts

THE LINUX FOUNDATION

OPENCHAIN

◆ORCRO

Capability Assessment

Five levels of development

1	2	3	4	5
Initial	Repeatable	Defined	Managed	Optimising

INITIAL: Minimal knowledge of open source compliance practice and procedure

REPEATABLE: Some steps towards compliance. Some systems in place, but application ad hoc

DEFINED/IMPLEMENTED: Policies, practice and procedure in place, but not necessarily in operation

MANAGED: Policies etc. in place, and in operation, and improved as considered necessary

OPTIMISING: Policies etc. in place, in operation, and actively managed using appropriate metrics and a process of continuous improvement.

Example Assessment Dashboard

Common framework and visual communication of strengths and development areas

Can be used across a community, organisation, supply chain for consistency of discussion

Development Planning

Visual clarity of priorities for development.

Can be used to create a 'Heat map' in response to key issues risks or ambitions.

Tool is available on the Open Chain github

Capability Model on GitHub

https://github.com/OpenChain-Project/Reference-Material/tree/master/Capability-Maturity-Model

Call for collaboration

- Join a meeting:
  - see https://openchainproject.org/participate
- Join an OpenChain mailing list:
  - https://lists.openchainproject.org/g/main
  - https://lists.openchainproject.org/g/education
- Contact us directly:
  - stephen.pollard@orcro.co.uk and andrew.katz@orcro.co.uk
  - Catch us in a bar/at FOSDEM/around Brussels
    - Andrew: +44 7970 835001 (What's App: if I'm sharing my location, feel free to track me down)

Andrew Katz
CEO - Orcro Limited

andrew.katz@orcro.co.uk

Stephen Pollard
Director - Orcro Limited

stephen.pollard@orcro.co.uk

Capability Model