Navigating Open Source Governance

Eric Tice
Global Open Source SME Lead, EA
Wipro Technologies

@EricTice4
Who we are today

$8.1B Global revenues*

Silicon Valley Innovation Center

Technovation Center in Bangalore

25k+ open source developers

Developers

Foundation

Partners

Customers

kubernetes

ONAP

EDGX FOUNDRY

Drupal

wipro digital

wipro ventures

wipro holmes

Designit

topcoder

APPIRIO

cellent
Why Do I Need Governance In Open Source?

- Get all the benefits from adoption
  - Innovation
  - Flexibility
  - HR
  - TCO

- Addresses core complexities of Open Source adoption

- Risk management and mitigation
  - Security
  - Licenses
  - Versioning
Agenda

• Open Source Challenges and Considerations
• Open Source Adoption
• Open Source Strategy
• Open Source Governance
  – Case for Open Source Governance
  – Define your Open Source Strategy
  – Adoption Considerations
  – Building a Governance Model
Open Source evolution

• Many organizations early on would not allow Open Source
• Developers push to include Open Source to drive innovation and improve efficiency
• Ops migration to Linux from traditional Unix or Mainframe
• Business buy in and adoption of processes to drive strategy to reduce cost and improve time to market

Generation I
Generation II
Generation III (Netflix)
Generation IV (Capital One)
According to the Red Hat Open Source Survey there has been an 69% increase in usage *since April of 2018*

Adoption of Open Source to support industry trends like cloud, serverless and microservices technologies

Even Microsoft has jumped headfirst into the pool announcing its commitment to Open Source and acquiring GitHub

Companies like IBM recently acquiring Red Hat, Salesforce purchasing Mulesoft, and beginning to narrow the commercial OS vendor field
Challenges and Misconceptions in Open Source Adoption – Yesterday and Today

• Historically many enterprise processes required strict adherence to commercially licensed software
• Lack of adequately trained resources in Open Source
• More tools means more management
• Integration with proprietary tools can be difficult
• Support model: community vs vendor
• Open Source provides instant cost benefit
• Open Source is not secure because it is community driven
• Open Source is not stable
• Licensing is licensing. No different than proprietary software right?
• Commercial is not Open Source
  • Community vs Commercial vs Proprietary
IT Governance

- Processes and methodologies to enable an organization’s strategic business goals through defined IT services, software and infrastructure.
- Reduces potential risks related to lack of policies, processes and standards across the enterprise.
Open Source Considerations

- Open source may not be the immediate cost benefit expected
- Patches and upgrades are frequent and often faster than proprietary
- Lack of properly inventoried Open Source tooling across applications can lead to integration, security, license and maintenance issues
- Vulnerabilities are not Open Source issues but more a lack of adequate patching and oversight
- Open Source licensing complexities can cause major issues if not managed properly
- Selecting the best support model depending on available skills vs cost of support
The Case for Enterprise Open Source Governance

- Although there are reportedly 20 main Open Source licenses used by nearly 98% of the Open Source and OSI has approved 82 licenses, companies such as Black Duck have found as many as 2500 available on the internet.

- Company implementations of Brown or Red shift projects will see an increase in Open Source and Cloud adoption.

- Often Open Source tools are a vast pool of possibilities with variant community involvement.

- Do you know how many different groups are implementing Open Source in your organization?
Open Source and Security

• Most vulnerabilities can be found in software, be it proprietary or Open Source or custom due to lack of patched software
• Community Open Source is typically faster to address and release patches than large proprietary software

Vulnerabilities

Vulnerabilities in Top 100 Projects

Vulnerabilities over 10 yrs old

*Blackduck

*Whitesoure

*Whitesoure
Open Source Repository Management

- Community vs Commercial versioning
- Patches and features not considered stable by Supported Commercial Vendor
- Product of release cycles in a commercial world
- Governing teams usage of versions to assure issues with stability is key
- Manage a set of governance tooling to track versions of all used software and licenses to assure stability and compliance
- Security vulnerability / CVE tracking and mitigation
Is your Organization Ready for Open Source?

- Developers often drive the use of Open Source without collaboration or alignment to business strategy
- Siloed groups within the organization
- Security groups often shut down Open Source without support
- Culture ready for change
- Existing Governance processes?
Offering Open Source, Protecting Your Offering

• You have decided to be an innovator and offer to the community

• Do you throw it out on GitHub and hope for the best?

• Open Source doesn’t mean you can’t still have proprietary IP

• Open Source IP handled through appropriate licensing and copyright
  • Software is generally copyright protected
  • Licensing gives permission for use and redistribution and controls contribution

• Processes for managing use of code through licensing agreements or auditing GitHub downloads
Building a Governance Model

Organizational Structure
1. Build Business Road-map
2. Determine current Open Source utilization
3. Defined Operation Model
4. Clear Roles and Responsibilities for Stakeholders
5. Defined metrics and KPIs
6. SDLC of services

Policies and Standards
1. Defined Best Practices for managing Open Source
2. Development Standards
3. Define Team ownership
4. Communication Policies
5. Defined owners of enforcement of policies and standards
6. Change Management Policies
7. Building guidelines for COE
8. Contribution policy
9. Community/ecosystem engagement models
Building a Governance Model (cont.)

Risk Assessment and Mitigation plan
1. Assure compliance with state and federal regulations where applicable
2. Defined and implemented Information Security practices
3. Risk Mitigation Strategy clearly defined
4. OS management and framework governance
5. Rollback and failure plan for Automated CI/CD
6. Defined Continuous monitoring plan for all Open Source software and hardware

3rd Party Management
1. License management
2. 3rd party audit of internal Open Source components
3. Assess Legal compliance by Vendors
4. Define processes for upgrades, patches and regular maintenance
5. Support model selection policy
Resources

Documents
1. 2019 Open Source Security and Risk Analysis by Synopsis Cyber Security Research Center and Black Duck
3. Gartner and Forrester annual reports on Open Source

Acknowledgements

Thank you to the following people for review and recommendations
• Andrew Aitken, GM & Global Open Source Practice Leader at Wipro, @AitkenAndrew
• Sreekanth Nymars, Open Source COE Lead at Wipro
• Gilles Gravier, Director & Senior Advisor Open Source and Blockchain, @gravax
OPEN SOURCE SUMMIT
NORTH AMERICA

THE LINUX FOUNDATION