

Corporate Open Source Software Compliance

Building Practical Strategies

Tuesday
05 April 2005



Holme Roberts & Owen LLP
Attorneys at Law



Disclaimer and Rights

This presentation is intended for general informational purposes only and should not be construed as legal advice or legal opinion on any specific facts or circumstances, nor is it intended to address specific legal compliance issues that may arise in particular circumstances. Please consult counsel concerning your own situation and any specific legal questions you may have.

The thoughts and opinions expressed in this presentation are those of the individual presenters and do not necessarily reflect the official or unofficial thoughts or opinions of their employers.

For further information regarding this presentation, please contact any of the presenters listed on the following slide.

Unless otherwise noted, all original content in this presentation is licensed under the Creative Commons Attribution-Share Alike 3.0 United States License available at: <http://creativecommons.org/licenses/by-sa/3.0/us>.





Overview

What We Will Cover

Objectives for the Compliance Plan

Initial Audit and Risk Profile

Compliance Program

Compliance team

Policies and controls

Education

Enforcement

Maintenance and Update

Best Practices for Implementation



Establishing Objectives

What Do You Want to Achieve?

- Increasingly unrealistic to avoid the use of OSS entirely
- Knowledge and compliance are more practical objectives

Make each use of OSS

an intended use of OSS

and a compliant use of OSS

- Control entry of OSS into the organization
 - Direct – Internal development and IT organizations
 - Indirect – Third party software and outsourced development
- Control the release of OSS by the organization
 - Release of existing code under OSS licenses
 - Contributions by developers to OSS projects
 - Licensing of OSS included in proprietary products



Establishing Objectives

What Else Will You Achieve?

- Beyond knowledge and compliance
- Consider added strategic benefits
 - Increase understanding of benefits of OSS
 - Facilitate increased communication regarding OSS
 - Build knowledge of available OSS solutions
 - Build relations with OSS community
 - Develop marketing and public relations edge
 - Preparation for anticipated acquisition, sale, or new product or service release



Initial Audit and Risk Profile

Understand and Evaluate the Risks

- Audit process should be tailored to fit your organization
- Goals will remain common
 - Scope of use
 - Nature of use
 - Existing policies, procedures and agreements
- Work to understand costs and risks posed by OSS to your organization (including those unique to your organization)
- Balance benefits and advantages against costs and risks
 - Do the costs and risks you are willing to accept vary (e.g., based on product, market, other factors)?
 - At what point do other options become superior? (OSS vs. proprietary licensing vs. build it yourself)
- Use results to shape overall OSS strategy (e.g., if the audit shows a large number of existing uses, design strategy to handle a high volume of requests)



Elements of a Compliance Program

Core Elements of a Successful Program

Compliance team

Policies and controls

Education

Enforcement

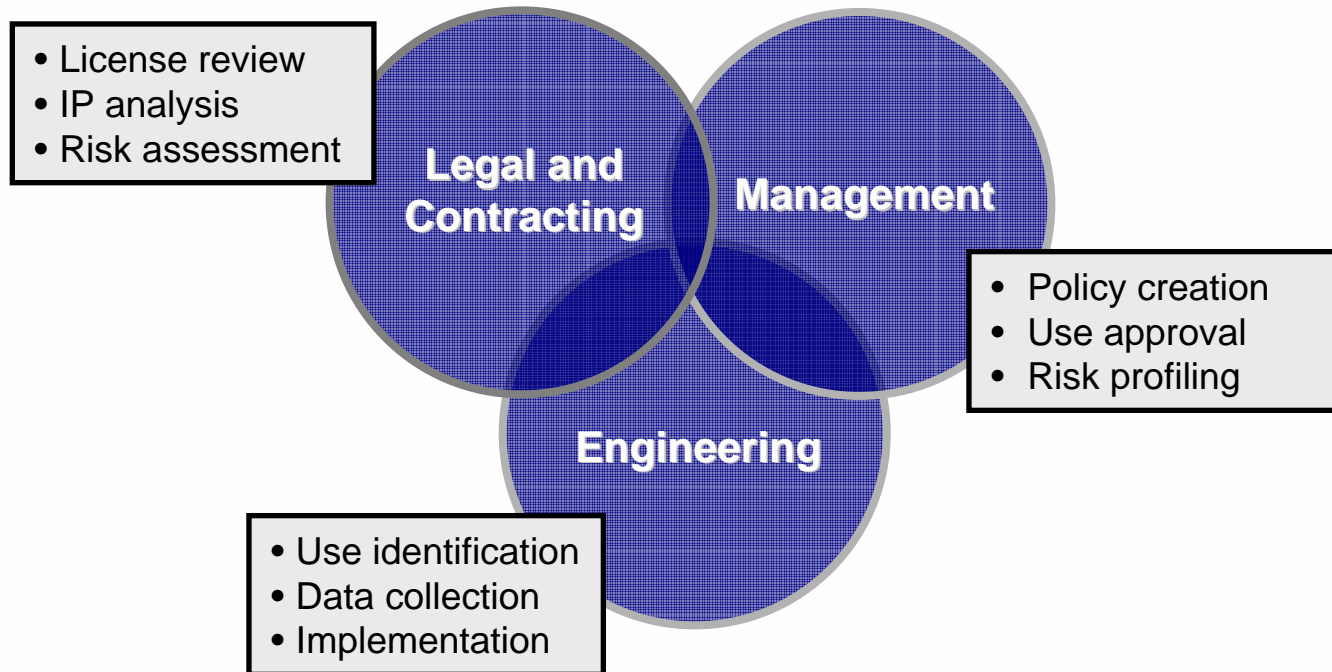
Maintenance and Update



Elements of a Compliance Program

Building an OSS Compliance Team

- Cross-disciplinary group



- Defined role/purpose
- Strong and open mandate from management
- Recognized leadership



Elements of a Compliance Program

Compliance Team is the Central OSS Authority

- Central source for awareness and expertise regarding all open source activities within the organization
- Central point of contact on OSS
 - Within organization - Defining and understanding issues
 - Outside organization – Communications, marketing, and licensing
- Directs compliance efforts of various business and project teams
- Defines and manages ongoing OSS compliance program and review process



Elements of a Compliance Program

OSS Management Policies and Controls

- OSS policies and controls should be developed as they would be for other forms of licensed software. . . .

“Vendors have to comply [with OSS licenses], just like they would have to with any other proprietary software license.”

Harald Welte,
Chairman of 
firewalling, NAT and packet mangling for Linux 2.4

. . . but with the appreciation that OSS poses unique issues not posed by other forms of licensed software.

“[T]he acquisition and use of FOSS necessitates implementation of unique risk management practices.”

 *IT Examination Handbook*



Elements of a Compliance Program

OSS Management Policies and Controls

OSS is unique

Traditional policies are inadequate

- Existing policies and controls are likely inadequate for OSS
 - Significantly different from proprietary software
 - Even the best existing policies likely leave gaps
- Use knowledge of issues obtained from OSS audit
- Establish policies and controls to deal with these issues
 - Review and track existing and future OSS use
 - Review and approval process for OSS usage proposals
 - Ensure implementation of OSS compliance plans and requirements
- Document policies
- Maintain central records



Elements of a Compliance Program

Education

- Essential to raising awareness of OSS policies and strategies
- Include all stake-holders (development, management, procurement, and legal)
- Build a common understanding
 - Issues and facts of OSS licensing
 - Business and legal risks of OSS
- Publicize and promote the compliance process within the organization
- Promote a “culture of compliance”
- Formal and informal methods
 - Education sessions
 - Periodic memoranda on developing issues
 - Information sharing among and between interested groups



Elements of a Compliance Program

Enforcement

- Enforce policies on projects known to be using OSS
 - Were policies observed?
 - Has use changed over time?
- Periodic reviews for new OSS usage in other areas
- Focus attention on distribution, production, and any use
- Work to facilitate a consistent policy implementation
- Is appreciation of the issues sufficiently complete in the individual business units involved with OSS?



Elements of a Compliance Program

Ongoing Management and Update

- Your use of OSS is likely not static
 - Changing uses of existing OSS
 - New uses
 - New product and service offerings
 - Acquisitions and divestitures
- The OSS community is also not static
 - Legal risks
 - Licensing and interpretation environment
 - IP infringement landscape
- Your compliance policies and procedures should not be static
- Build periodic reviews and updates into the program while maintaining consistency



Best Practices for Implementation

Key Recommendations

- Keep it simple (and consistent)
- Work within existing procurement and licensing infrastructures, but be prepared to establish new infrastructure
- Clearly document policies
- Operate in real-time (avoid historic analyses)
- Audit and re-audit
- Re-train regularly through ongoing education
- Periodically review and adjust program accordingly

Thank You.



Holme Roberts & Owen LLP
Attorneys at Law