



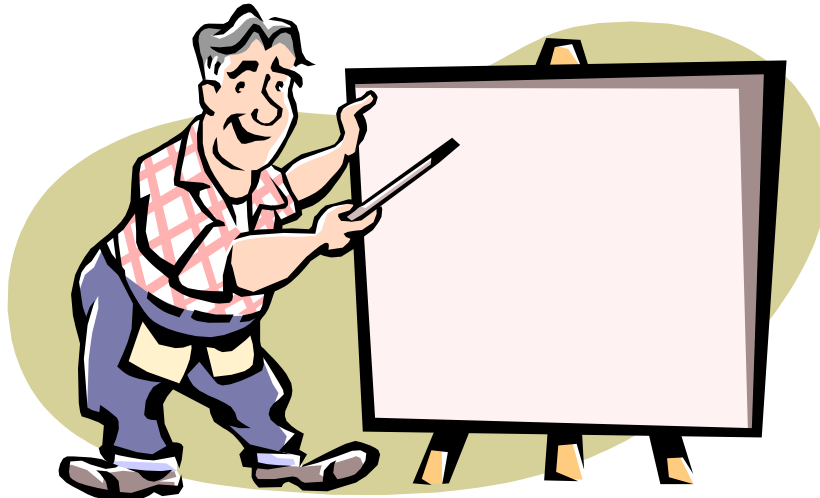
Practical Guide to Implementing an Open Source Compliance Program

Dr. Philip Koltun
The Linux Foundation



Goal of this talk

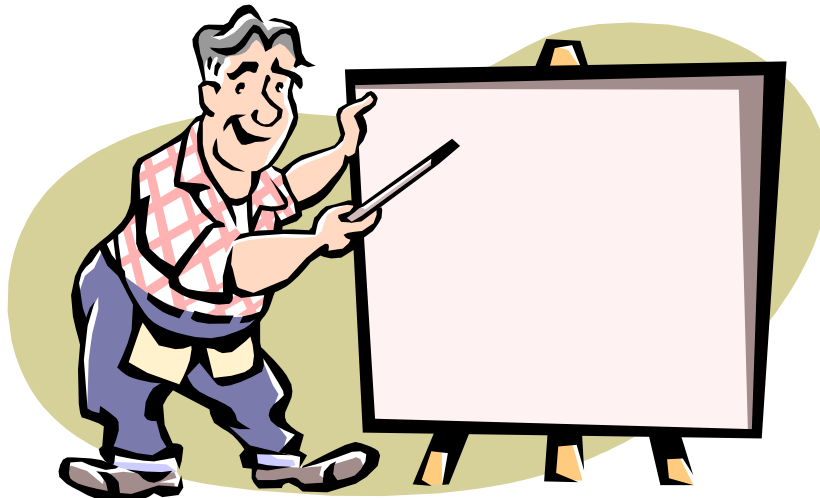
- To tell you about new resources available through the Linux Foundation that will help companies with their open source compliance efforts





Topics

- Short background on open compliance problem
- Open compliance process in a nutshell
- Challenges in implementing the compliance process
- Resources available from The Linux Foundation





Some companies still don't get it ...



Software Freedom Law Center

[Team](#)[News and Activities](#)[Services](#)[Publications](#)[Blog](#)[Oggcast](#)[Contact](#)[Donate](#)

December 14, 2009

Best Buy, Samsung, Westinghouse, And Eleven Other Brands Named In SFLC Lawsuit

Evidence of GPL Violations and Copyright Infringement Found in TVs, DVD Players, and Dozens of other Electronic Devices

New York, NY, December 14, 2009//Best Buy, Samsung, Westinghouse, and JVC are among the 14 consumer electronics companies named in a copyright infringement lawsuit filed today in New York by the Software Freedom Law Center (SFLC).

The SFLC is a non-profit law firm established in 2005 to provide pro-bono legal services to Free and Open Source Software (FOSS) developers. The



Why is compliance effectiveness important?

Compliance can be a labor-intensive activity

- Identifying all components
- Investigating provenance
- Compiling license and attribution notices
- Preparing packages for posting to portals
- Etc.

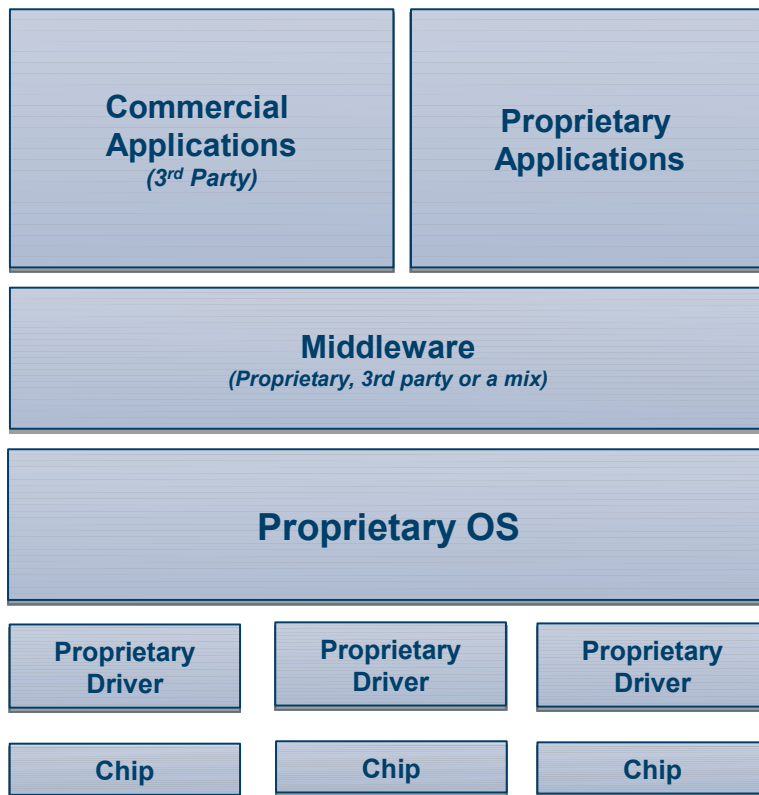


Ineffective compliance can jeopardize product shipment schedules and increase costs up and down the supply chain

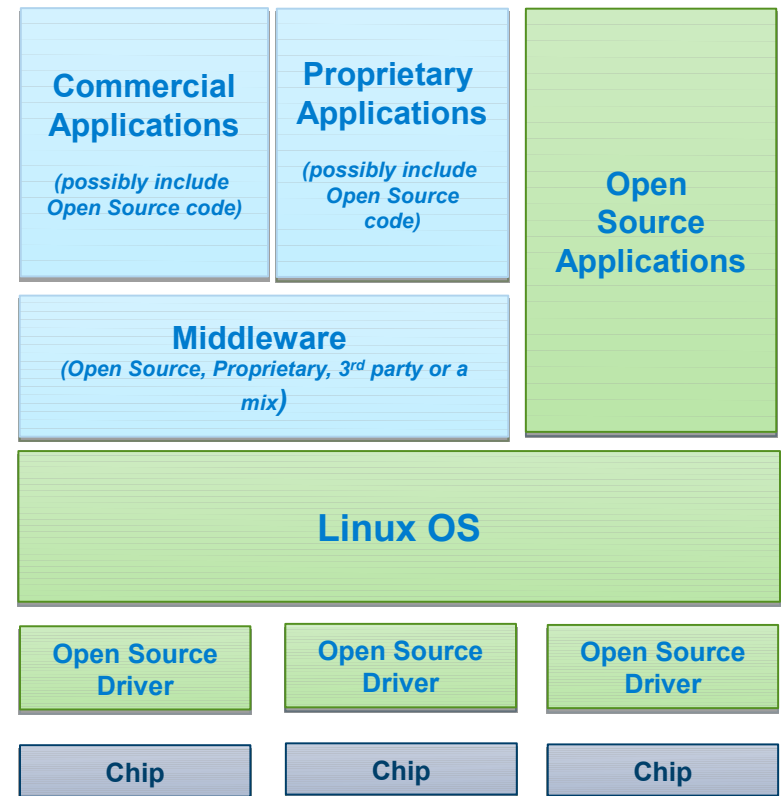


Product development relies now on open source

From



To





But use of open source software carries obligations

- OSS license obligations generally are triggered *only* when external distribution occurs.
- Obligations could consist of:
 - Inclusion of copyright and license in the
 - source code and/or product documentation
 - or user interface.
 - Disclaimers of warranty by the authors
 - Notices as to source code availability
 - Etc.



Analysis performed during review of intended open source use will clarify obligations

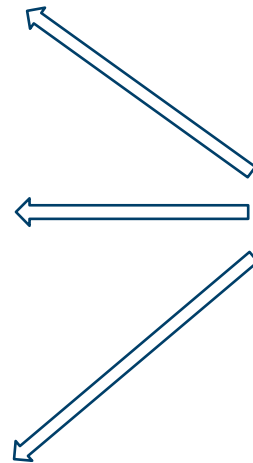


The Compliance Process in a Nutshell

Core Compliance Processes



Supporting Elements





Seems pretty straightforward, doesn't it?

- It is – or could be – but there are a few nuances and challenges that could complicate matters. So:



- Some questions for organizations to ponder

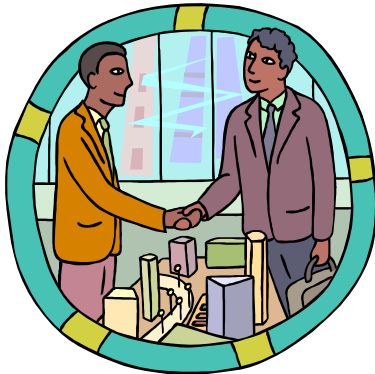


Why is open source discovery a challenge?

- What really goes into a product planned for external release?
 - No Bill of Material
 - Original authors are gone
 - Source code base is very large
 - Many product versions and software versions
 - Third party software in binaries only
- Manual code audits are time-consuming and potentially inaccurate
- Code scans might be costly and involve much follow-up



What about getting your software suppliers to disclose their inclusion of open source?



- Did they perform due diligence? Are their disclosures complete and accurate?
- Should you rely on standard license warranties?
- Should you demand a commercial scan? Can you demand they give you source code for you to scan?
- Once they've disclosed open source, have they given you what you need to satisfy *your* obligations once your product ships?



What makes Review and Approval difficult?

- Availability of architectural diagrams
- Skilled reviewers
- Sufficient staff time
- Role of the OSRB
- What's safe, what's risky?





What challenges exist in satisfying obligations?

- Capturing the right source code
- License text, copyright notices, attributions, etc.
- Supplier responsibilities
- Posting code to portals
- Doing it all early and fast enough





Are there compliance challenges in approving community contributions?

- Aligning contributions with company interests
- Protecting company IP
- Distinguishing individual vs. company contributions
- Reviewing contributor license agreements





More issues to think about ...

- How and where are open source compliance activities injected into existing business processes?
 - Product planning and product authorization
 - Project planning and scheduling
 - Architectural design review
 - Documentation
 - Verification
 - Release readiness review
 - Etc.

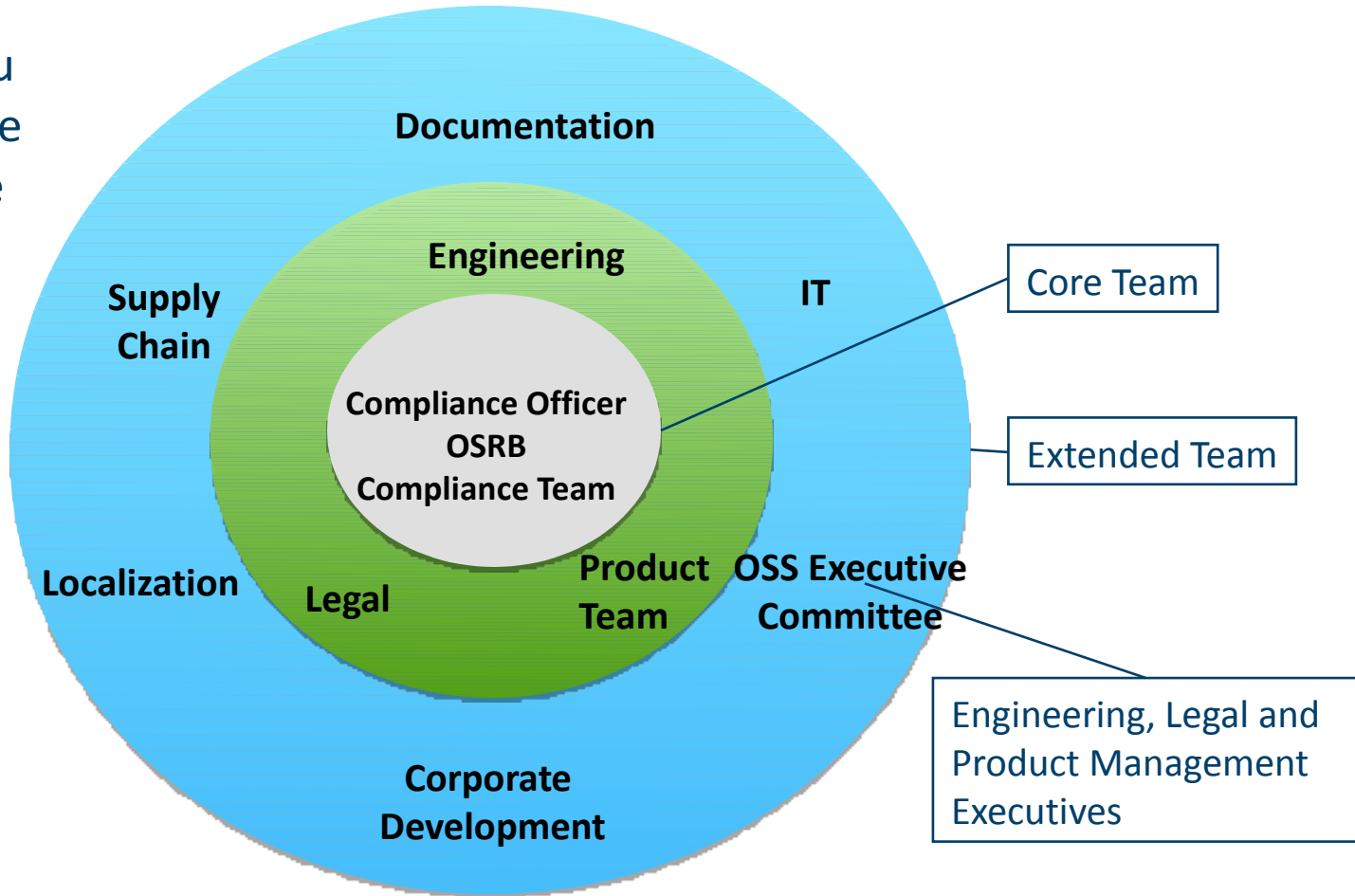


→ Treat compliance as one more type of project activity to be routinely planned and executed.



More issues to think about ... (continued)

How do you organize the compliance function?

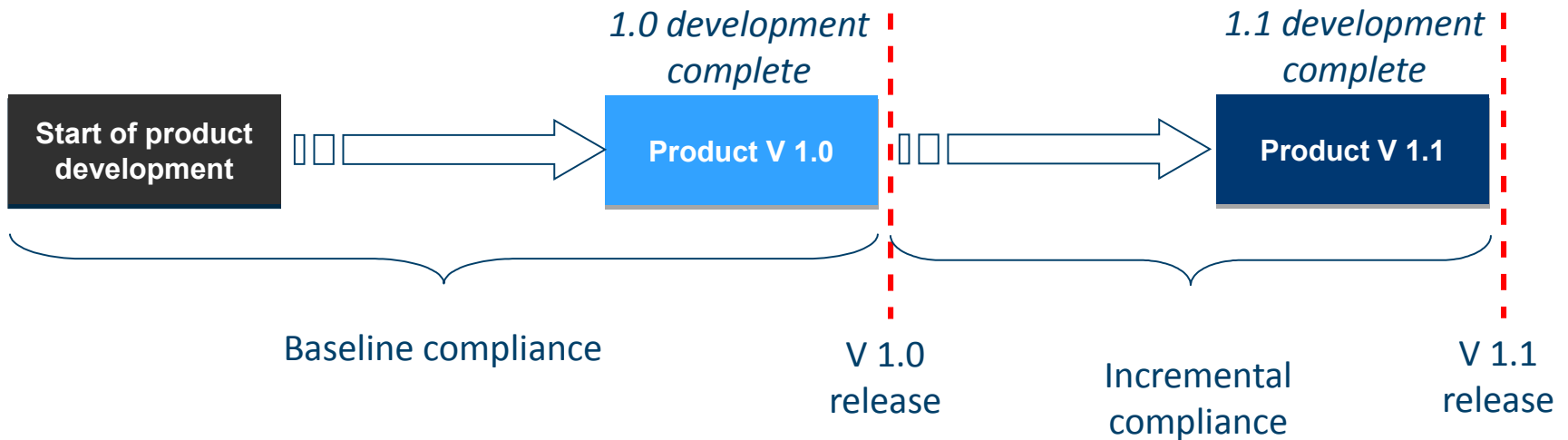




More issues to think about ... (continued)

What are your priorities for compliance and what's your plan?

- Establishing initial compliance, then doing incremental compliance





More issues to think about ... (cont'd)

- In what ways can the compliance process fail (and how can we prevent those failures through compliance activities)?

→ Conduct a Process FMEA

What are the failure modes and how could those failures occur?

- Intellectual Property FOSS failures
- FOSS license compliance failures
- Compliance process failures
- Etc.





Paradox

- Companies could benefit from communicating openly about their compliance practices and challenges but are reluctant to do so.



The Linux Foundation is a unique resource for training, tools, and guidance to people with compliance responsibilities.



Why is the Linux Foundation focusing energy and resources on compliance?

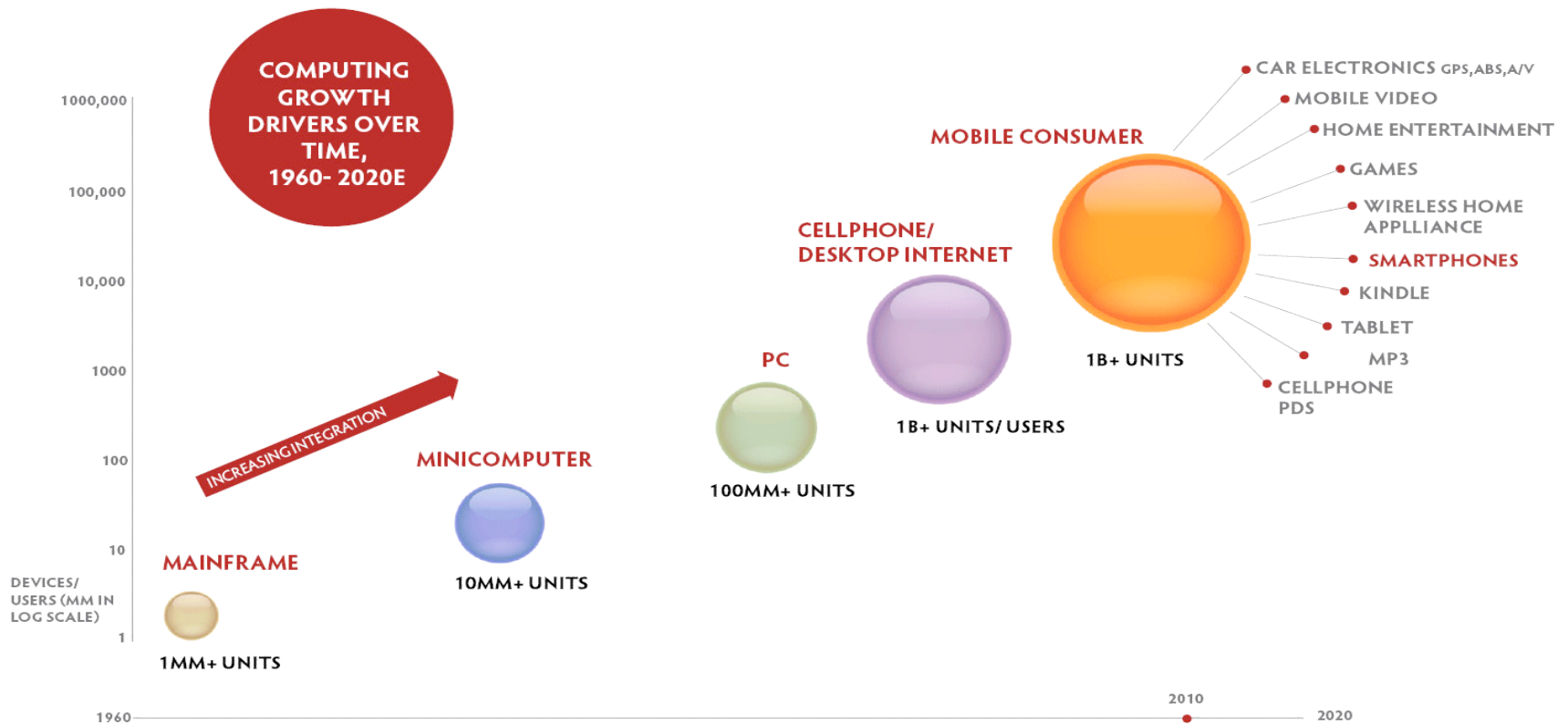
- It is in our core mission:



- We have the highest visibility among open source legal organizations and can unify legal efforts and communicate those efforts to the press and public
- Our workgroups (FOSSBazaar and SPDX™) and events (Legal summits, Collaboration summits and LinuxCon) already bring together developers, community legal resources and industry
- We have valuable intellectual property in this area to share with the industry and community



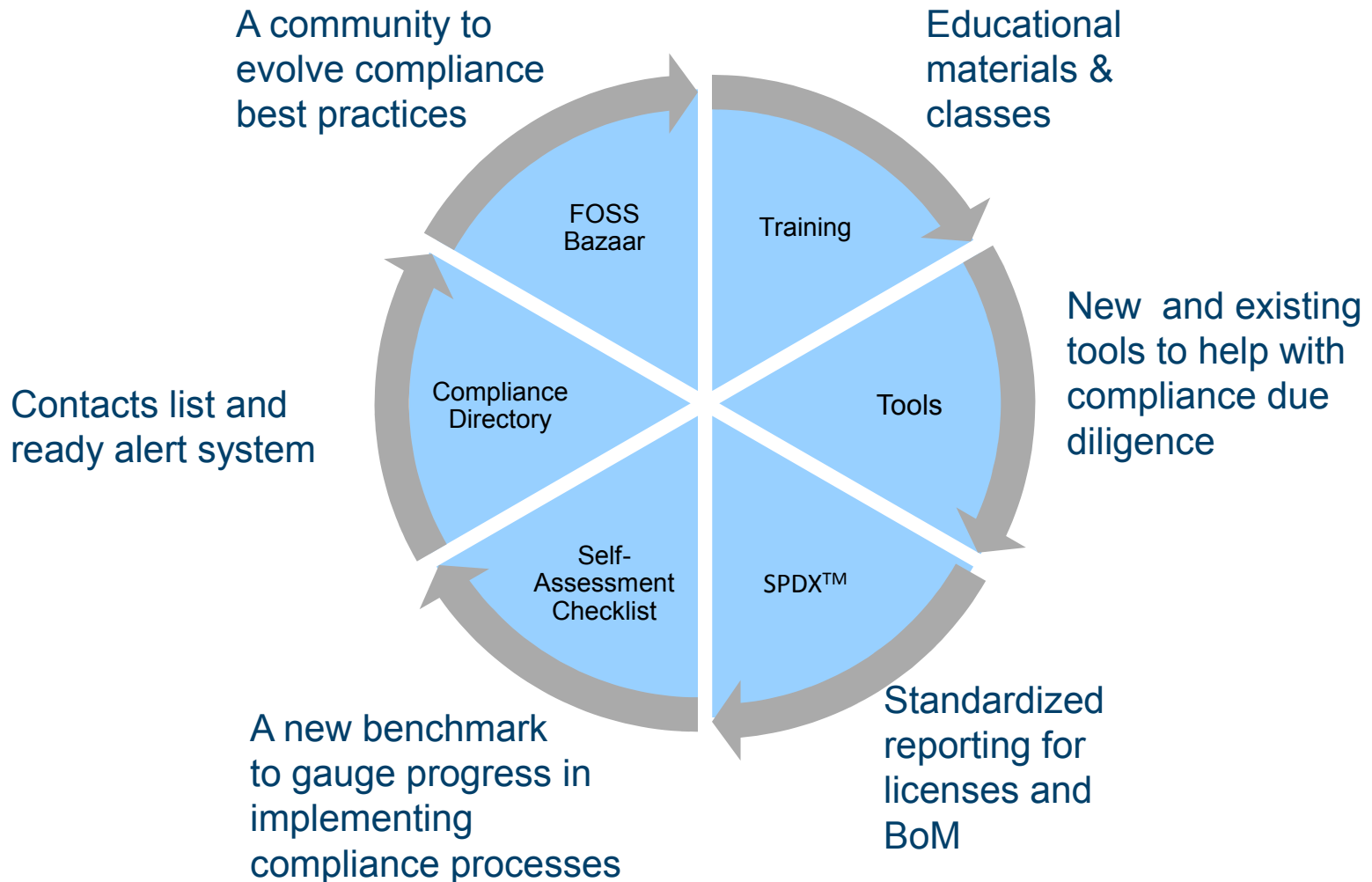
Why now? Because the number of companies using open source to create products is exploding.



Morgan Stanley Research 2010



The Linux Foundation has created a new program focus to help: The Open Compliance Program





What will the Open Compliance Program accomplish?

- Increase awareness of compliance and help bridge the disconnect between companies, legal community and the developer community.
- Make compliance easier
- Decrease FUD around Linux & open source
- Standardize some compliance aspects
- Increase the number and availability of open source compliance tools
- Provide a forum for compliance improvement efforts





Linux Foundation now offers compliance training

Training modules cover the operational details of open source compliance activities and can be tailored for different audiences.

Course#	Title	Length
LF281	Executive Review of Open Source Compliance	Half-day
LF384	Overview of Open Source Compliance End-to-End Process	One day
LF488	Implementation and Management of Open Source Compliance	Two days

See <http://training.linuxfoundation.org/courses>

Who should be trained about open source compliance?

- Those who bring software into the organization, develop and distribute products, and interface with customers and suppliers
- Includes
 - Corporate Management
 - Engineering
 - Product Management, Project Management, and Process Management
 - Testing, Quality Assurance, Configuration Management and Logistics
 - Law Department
 - Purchasing / Supply Chain
 - Information Technology
 - Marketing, Sales, and Customer Support



A robust training program reduces the likelihood of a compliance problem and demonstrates good faith and diligence in educating corporate staff



We have free white papers on compliance available now

Sign Up for the Free Linux Foundation Publication

Free and Open Source Software Compliance: The Basics You Must Know

Publication: "Free and Open Source Software Compliance" by Ibrahim Haddad (Ph.D.), The Linux Foundation

Available Now

This white paper is a first in a series that will focus on the various practical aspects of ensuring free and open source software compliance in the enterprise. This paper provides basic discussion on the following topics:

- The changing business environment moving to a multi-source development model
- The objectives of compliance and the benefits resulting from having a successful compliance program
- The consequences of non-compliance with the licenses of free and open source software
- The compliance failures that can occur, how to avoid them and prevent them from happening in the future
- The lessons learned from the various non-compliance cases with emphasis on the positive learnings



About the Author (Ibrahim Haddad, Ph.D.)

Ibrahim Haddad is Director of Technology and Alliances at the Linux Foundation focusing on Mobile Linux initiatives and advancing the Linux platform for next-generation mobile computing devices.



Sign Up for the Free Linux Foundation Publication "Free and Open Source Software Compliance: The Basics You Must Know"

First Name: *

Last Name: *

Email: *

Phone Number: *

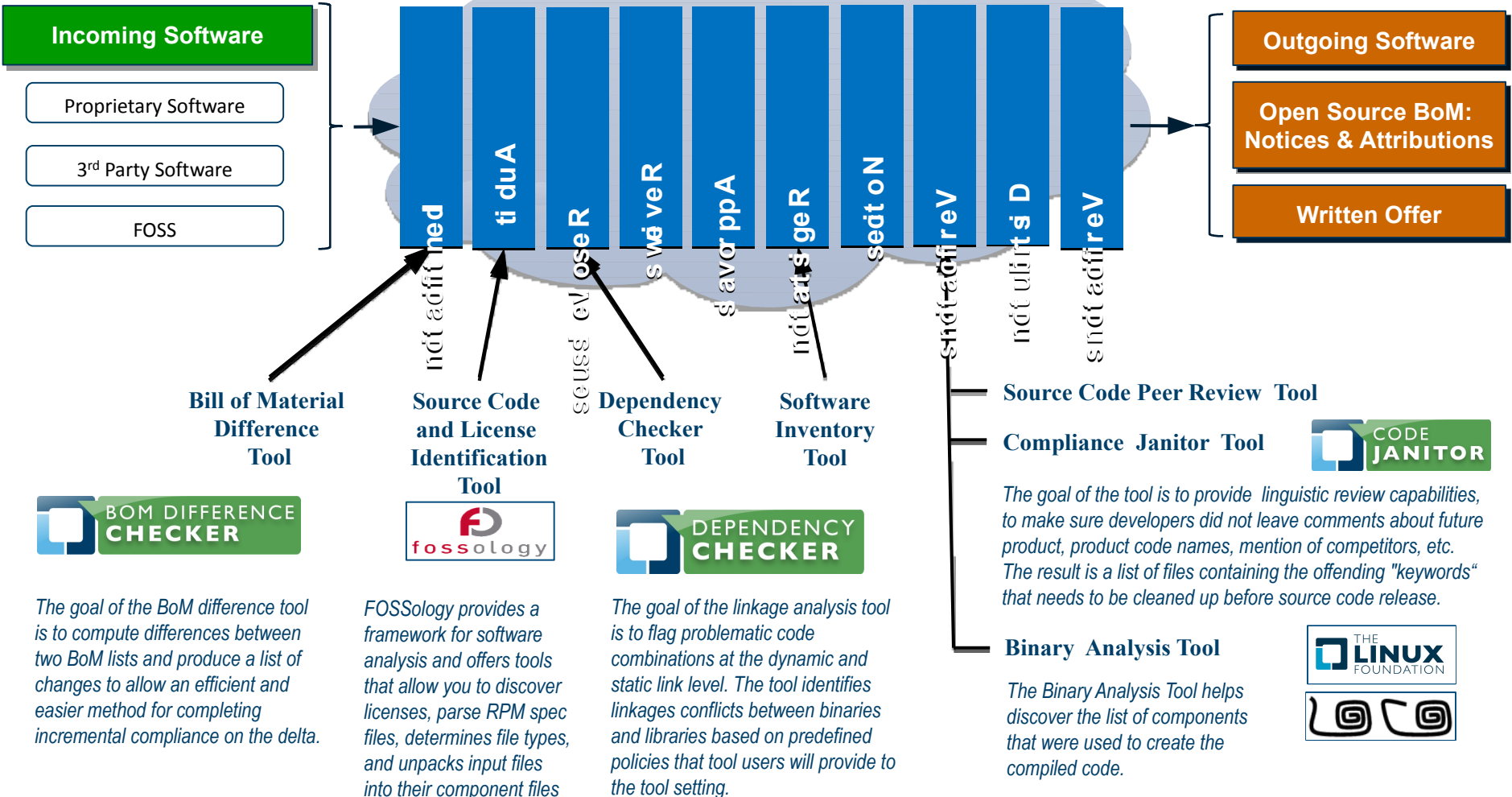
Title: *

Company: *

[View our Privacy Policy.](#)



LF tools are designed to be practical and easy to fit into a simple FOSS compliance process





The Linux Foundation has created new compliance tools to supplement existing ones

- **Dependency Checker Tool**
 - Identifies combinations at the dynamic and static link level
 - Offers a license policy framework that enables Compliance Officers to define combinations of licenses and linkage methods that are to be flagged if found as a result of running the tool.
- **Bill of Material (BoM) Difference Tool**
 - Computes differences between two BoMs to allow an efficient and easier method for completing incremental compliance.
 - Based on standardized way of reporting FOSS included in a commercial product.
- **Code Janitor Tool**
 - Flags keywords that should be scrubbed from the source code before it is released to the public (such as future product names, email addresses, derogatory comments, etc.).



... and will list other open source and commercial compliance tools on a forthcoming resources page

Examples of open source tools

- **FOSSology**
 - Facilitates the study of FOSS and to discover and report FOSS licenses.
 - Provides a framework for software analysis and offers tools that allow you to discover licenses, parse RPM spec files, determines file types, and unpacks input files (such as .tar, .gz and .iso) into their component files
- **Binary Analysis Tool**
 - Scans binary files and provide information if the binary was built using open source software.
 - A community tool available at binaryanalysis.org
- **OSS Discovery**
 - A scanning tool that helps enterprises find the open source software included in their internal applications and installed on corporate workstations and servers. OSS Discovery is available from OpenLogic.

If you know of other open source tools that should be listed or wish to have your commercial tool listed, send info to compliance@linuxfoundation.org.

The Need



We need a standardized, adopted format for a software Bill of Materials



- Package contents evolve over time
 - Different versions can have different licenses
 - Declared license of a package is not always accurate
 - Package with different license has “useful” routines (that potentially get included)
 - Different versions can have different licenses at the file levels
- Package dependency/requisite hierarchy can have incompatibilities
 - Hidden/enveloped package in dependency chain
 - Incidental packages get included by accident
 - All OSS licenses not compatible with each other



- Phase 1: Standardize on way of encoding the information about a package (.rpm, .tar, etc.) so that it can be:
 - Uniquely identified (single file change, versions, etc.)
 - Machine & Human - readable/creatable
 - Information needed by compliance teams is present
 - Source for analysis is clearly identified
- Phase 2: Determine ways the package facts can be publicly shared.
 - Easy to look up and share - common site and/or embedded in package
 - Neutrality, issues publicly visible (and can be fixed), in advance of distribution deadlines
 - Does not rely on author, others can generate
 - Specification verification tools - does a file comply?

- Open Source Org's
- End-Users
- Integration & Services
- Device OEMs
- Applications
- OS Distributions
- Systems
- Semiconductor Vendors



...and others

Participation is from a range of organizations and across various roles



- Define a file format for license and copyright information to accompany packages
 - Guiding Principle: **Just the facts – no interpretations**
- Define a standardized short form to refer to the official version of common licenses
- Benefits
 - Allows easy exchange of license information between companies reducing burden on both suppliers and consumers
 - Avoids due diligence redundancy where the same source code package is analyzed multiple times by different receivers
 - Provides a unified method for exchanging license information



- 1 - Rationale
- 2 - Identification Information
 - Meta data to associate analysis generation methods and results with a specific package
- 3 - Common Overview Information
 - Facts that are properties for entire package
- 4 - Non-standard License Detected
 - Full text list of any license that can't be matched
- 5 - File Specific
 - Facts that are specific to each file included in a package

Appendix I - Recognized License Short Forms



Identification Information

- Version of SPDX™ specification used
- How this info was generated
 - Manual review (who, when)
 - Tool (id, version, when)
- Independent audit
 - “signed off”/”reviewed by” equivalents



- Formal Name of Package
 - Full name given by originator and version information.
- Package File
 - Name package obtained under (.tar, .rpm, etc.)
- SHA/HASH
 - Need independently reproducible, agreed on, mechanism.
 - Need to determine if any file changed and not match.
- Declared Published Location (download URL)
- Declared License for Package
 - Standardized and explicit versions as needed.
- Detected Licenses
- Declared Copyright Date and Holder/Licensors of Package
- Description of Package (optional)



File Specific Content

- File Name (including subdirectory)
- File Type (source, binary, archive)
- License(s) governing file (from file)
- Copyright Information dates and owners (if listed)

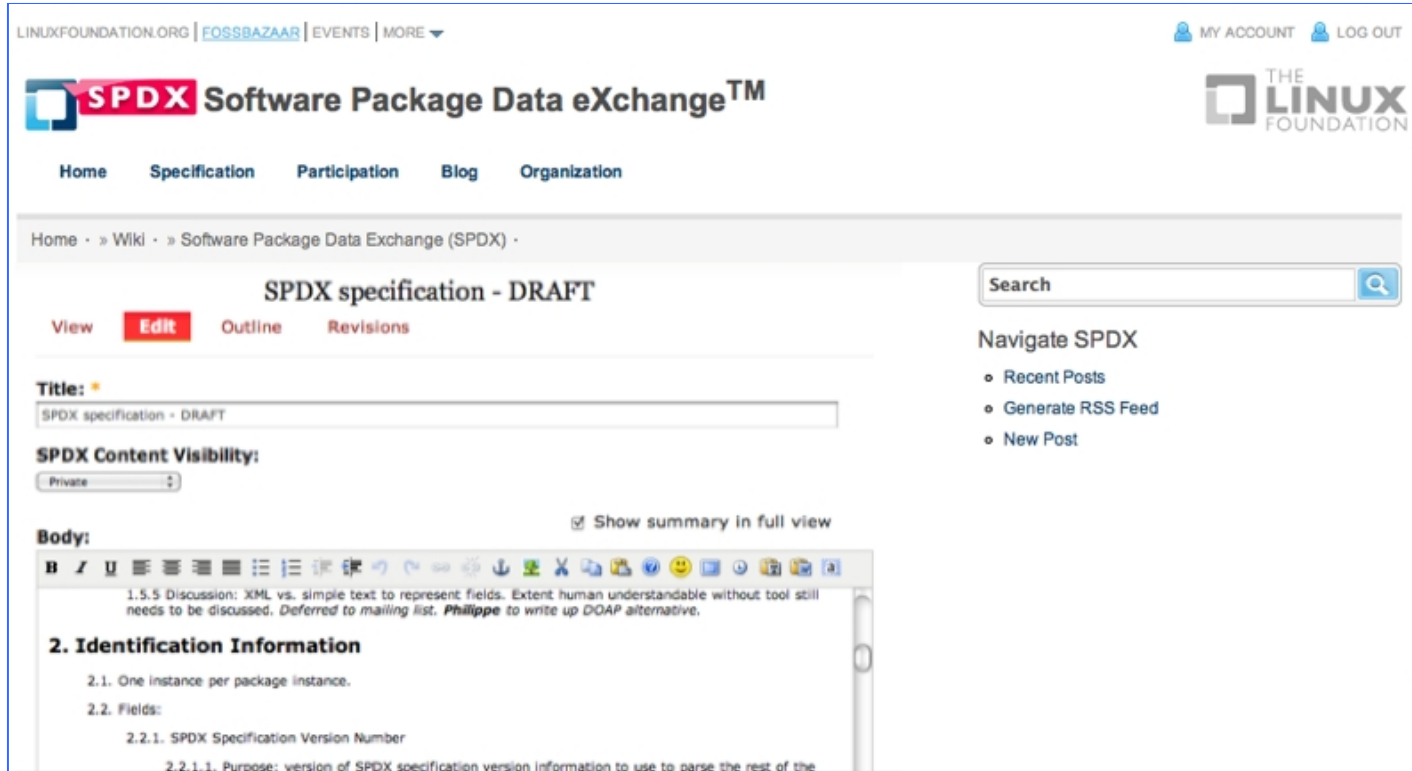


- Identifier assigned to be used inside package
 - If license found in multiple places, only one copy needed
- Full text of license discovered is reproduced



- Aim for ~90% coverage with standard short forms NOT exhaustive
 - Black Duck identified >1900 licenses in use
 - Appendix I currently has 112
 - ~20 licenses responsible for nearly all licensed open source projects
 - <http://www.blackducksoftware.com/oss/licenses#top20>
 - OSI ratified 80 licenses to be “open source”
 - <http://www.opensource.org/licenses>
 - Include common exceptions as separate short forms
- License names
 - Establish unique identifier for common open source licenses.
 - Evolve from Red Hat precedents and Debian’s Dep-5 proposals.
 - Pointer to official license text associated with name (URL)
 - Template version available to match against on SPDX.org

- Version 1.0 beta - available
- Soliciting testing and feedback

A screenshot of the Linux Foundation's SPDX website. The page title is "SPDX specification - DRAFT". The navigation menu includes "Home", "Specification", "Participation", "Blog", and "Organization". The main content area shows a rich text editor with a title field containing "SPDX specification - DRAFT" and a "Body" field containing text about XML vs. simple text and a section titled "2. Identification Information" with sub-sections "2.1. One instance per package instance." and "2.2. Fields:" with a sub-sub-section "2.2.1. SPDX Specification Version Number". The right sidebar contains a search box and a "Navigate SPDX" section with links for "Recent Posts", "Generate RSS Feed", and "New Post".



The Linux Foundation has developed a Self-Assessment Checklist

- The self-assessment checklist is offered to companies wanting to evaluate their compliance program against an extensive checklist set by the Linux Foundation that corresponds to recommended compliance practices.
- Self administered. The Linux Foundation will facilitate confidential company self-assessments upon request.

Optional:

- The Linux Foundation can provide recommendations to companies on how to implement missing or under-implemented elements in their compliance programs.





Sample practice from the Checklist

“The organization investigates the third party supplier's use of OSS and its OSS compliance practices as part of its supplier selection process.

- The organization investigates the third party supplier's compliance and supply chain management practices to evaluate their adequacy.
- The organization uses defined guidelines to determine if automated scanning or other confirmation of the supplier's disclosure is needed.
- Software license agreements include appropriate terms and conditions concerning OSS.
- Supply Chain staff and others who interface with suppliers have been trained in OSS matters and include OSS concerns in their discussions with third party suppliers.”



Compliance Directory and Rapid Alert System

- **Background**
 - Often when a violation is found or compliance inquiries are presented, it is difficult to reach out to the company in question because either the contact information for compliance is not published or it is difficult to find.
- **The Linux Foundation Solution**
 - The compliance directory is the “Yellow Pages” for compliance contacts. It will allow the Open Compliance Program to facilitate connections between open source developers and compliance contacts within a given company to discuss specific compliance questions. It also allows the Linux Foundation to communicate quickly with the community of compliance officers.

Software Freedom Law Center

December 14, 2009

Best Buy, Samsung, Westinghouse, And Eleven Other Brands Named In SFLC Lawsuit

Evidence of GPL Violations and Copyright Infringement Found in TVs, DVD Players, and Dozens of other Electronic Devices

New York, NY, December 14, 2009/Best Buy, Samsung, Westinghouse, and JVC are among the 14 consumer electronics companies named in a copyright infringement lawsuit filed today in New York by the Software Freedom Law Center (SFLC).

The SFLC is a non-profit law firm established in 2005 to provide pro-bono legal services to Free and Open Source Software (FOSS) developers. The suit was filed on behalf of the Software Freedom Conservancy (Conservancy), the non-profit corporate home of the popular software application BusyBox and many other FOSS projects, and Erik Andersen, one of the program's principal developers and copyright holders.

The First Rule of GPL Compliance: “Be Responsive When Contacted”

The SFLC has dealt with over a hundred compliance matters since its inception on behalf of various clients, including BusyBox and developers of significant portions of the GNU/Linux operating system. The vast majority of these matters usually end with violators voluntarily coming into compliance. In the rare cases when a company refuses to cooperate in good faith, the SFLC has been forced to take legal action on behalf of its clients to enforce FOSS requirements.

The SFLC continues to encourage companies to voluntarily come into compliance. “We always prefer cooperation” said SFLC communications director, Lysandra Ohrstrom. “We brought this suit as a last resort after each of these defendants ignored us or failed to meaningfully respond to our requests that they release the source code.”

The First Rule of GPL Compliance: “Be Responsive When Contacted”

The SFLC has dealt with over a hundred compliance matters since its inception on behalf of various clients, including BusyBox and developers of significant portions of the GNU/Linux operating system. The vast majority of these matters usually end with violators voluntarily coming into compliance. In the rare cases when a company refuses to cooperate in good faith, the SFLC has been forced to take legal action on behalf of its clients to enforce FOSS requirements.

Since 2007, the SFLC has sued six companies, including Verizon and Cisco, for selling products with embedded FOSS programs in violation of the GPL. Though the scope of this lawsuit is unprecedented in that it includes 14 defendants, the SFLC's primary goal is to encourage companies to join the software freedom movement, said Bradley M. Kuhn, Conservancy's president and the SFLC's technology director. “As embedded computer systems become more commonplace in everyday consumer electronics and more companies recognize the zero-cost licensing of Free Software over proprietary alternatives, it is more important than ever for manufacturers to learn to comply with the GPL”, Kuhn explained.

“The SFLC's objective, on behalf of its clients, is not only to ensure the freedom of FOSS code but to see that BusyBox's users get the full benefit of the software” Williamson added.

The suit was filed in the United States District Court for the Southern District of New York and will be heard by Judge Shira A. Scheindlin.

A copy of the complaint is available on our website.

For additional information or to arrange interviews, please contact SFLC communications director, Lysandra Ohrstrom, at (212) 461-1915 or by e-mail at lohstrom@softwarefreedom.org.

Other SFLC news...

Main Page | Contact | Privacy Policy | News Feeds


This page is licensed under the Creative Commons Attribution-NoDerivs 3.0 United States License. If you would like to make a derivative work of this page (e.g. a translation), please contact us.

SUPPORT SFLC


http://www.softwarefreedom.org/news/2009/12/14/buy-samsung-westinghouse-jvc-lawsuit/



The Open Compliance Directory compiles company compliance contacts

 US UK

[Home](#) [About Us](#) [News & Media](#) [Programs](#) [Workgroups](#) [Publications](#) [Events](#) [Training](#)

[Home](#) > [Open Compliance Directory](#) - Add Organization Request  [Logout](#)

Open Compliance Directory - Add Organization Request

In order to facilitate resolution of open source compliance issues short of contentious conflict, the Linux Foundation has compiled an Open Compliance Directory. The purpose of this directory is to identify corporate Open Source Compliance officers able to respond to compliance requests filed via the [Open Compliance - Request for Contact Information](#) web form. When a compliance contact request is received, the Linux Foundation Open Compliance Program will forward the request to the appropriate corporate contact listed in the directory.

Organization Information

Company / Organization Name: *	<input type="text"/>
Business Unit:	<input type="text"/>
Company / Organization Website: *	<input type="text"/>
Open Source Compliance Website: *	<input type="text"/>
Compliance Program Email: *	<input type="text"/>
Address: *	<input type="text"/>
City: *	<input type="text"/>
State: *	<input type="text"/>
Zip / Postal Code: *	<input type="text"/>
Country: *	<input type="text"/>
Contact Name: *	<input type="text"/>
Contact Email: *	<input type="text"/>
Contact Phone: *	<input type="text"/>

Compliance Program Information


Description of Program: *

Additional Compliance Notes:



- **A community of open source compliance practitioners that is complementary to the Linux Foundation in-house Legal Counsels community**

LINUXFOUNDATION.ORG | VIDEO | EVENTS | MORE ▾ MY ACCOUNT LOG OUT

 **Open Source Governance for the Enterprise** 

[Home](#) [News](#) [Blogs](#) [Resources](#) [Forums](#) [About Us](#)

FOSSBazaar

A Community For Free And Open Source Software Governance

FOSSBazaar is an open community of technology and industry leaders who are collaborating to accelerate adoption of free and open source software in the enterprise. Specifically, FOSSBazaar aims to:

- Expand upon the open source value proposition for a richer, safer, less expensive, better overall IT experience.
- Focus on free and open source software governance best practices, education and tools.



What's Hot!

- [Frequently Asked Questions](#)
- [FOSS Governance Fundamentals](#)
- [FOSSBazaar Videos](#)



Program Availability

1. **Training** **Available now**
 - Sign-up at: <http://training.linuxfoundation.org/courses>
2. **Self-Assessment Checklist** **Available Nov. 1**
3. **Tools**
 - FOSSology **Available now**
 - Dependency Checker Tool **Available now**
 - Code Janitor Tool **Available now**
 - Binary scanning tool **Available now**
 - Bill of Material difference tool **Available Q4 2010**
4. **SPDX™ Working Group** **Available now**
 - <http://spdx.org>
5. **Compliance Directory** **Available now**
 - <http://www.linuxfoundation.org/programs/legal/compliance/directory/>
6. **FOSSBazaar Community** **Available now**
 - <http://www.FOSSBazaar.org>



Your Support Is Crucial

- Help make compliance an institutionalized practice
- Get involved with working groups such as the SPDX™. Take part in the FOSSBazaar community.
- Enter your company's compliance contact info in the Open Compliance Directory.
- Recommend our training classes to your functional teams and suppliers that need to know more about compliance





Contact info

Philip Koltun, Ph.D
Director, Open Compliance Program
The Linux Foundation

pkoltun@linuxfoundation.org

or

compliance@linuxfoundation.org



Questions and Comments