» The Open Compliance Program

Self-Assessment Checklist

Version 1.0

November 2010

The Linux Foundation
http://www.linuxfoundation.org

Date	Version	Description
11/01/10	1.0	Initial release of the Self-Assessment Checklist

Preface

The Self-Assessment Checklist represents a key element of The Linux Foundation's Open Compliance Program, announced on August 10, 2010. The program also includes free tools to help with compliance due diligence, free education material, comprehensive professional training, an online compliance community (FOSSBazaar) to exchange compliance best practices, the SPDX™ (Software Package Data eXchange) standard for specifying an open source bill of material, and a compliance rapid response directory to help companies and open source developers connect on compliance matters.

Background

The Linux Foundation has compiled this extensive checklist of compliance practices found in industry-leading compliance programs. Companies can use this checklist as a confidential internal tool to assess their progress in implementing a rigorous compliance process and to help them prioritize their process improvement efforts. The Self-Assessment Checklist is constructed using at least two concepts from well-established models of process maturity such as the Software Engineering Institute's Capability Maturity Model:

- Process adoption progresses from initial process definition through institutionalization to a state of controlled process management. The goal of a compliance process, as with any process, is to achieve consistent and expected business results from its use. A checklist of recommended practices should prompt companies to assess the extent to which they've institutionalized compliance actions and the degree to which those actions produce needed business results
- A distinction should be made between process goals and the practices implemented to achieve those goals. The compliance checklist explicitly recognizes valid alternative practices that may be used to achieve a particular goal.

Compliance practices included in the checklist will improve the effectiveness of compliance programs as well as deliver tangible benefit relative to the cost of those practices. A process failure modes effects analysis (FMEA) approach has been used to identify the ways a compliance process can fail and practices to prevent those process failures.

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

Why is it called "Self-Assessment"?

This checklist is called "Self-Assessment" because organizations can use it internally without help from any third party and without exposing their internal compliance practices to anyone. The use of the checklist calls for a frank appraisal of a compliance program's strengths and weaknesses. Such judgments can best be made by members of the organization who are fully aware of the business unit's product development process, product roadmap, product architecture, and company culture. The checklist has no legal status or binding effect. Its use is entirely voluntary. Its sole purpose is to bring process gaps to light which will, if unaddressed, inevitably lead to compliance problems.

Audience and Intended Purpose

This document is intended for use by teams responsible for defining, implementing, and improving open source compliance programs within their organizations. Those just starting down the road of establishing a compliance program will especially benefit from The Linux Foundation's training courses on Open Source compliance rather than relying solely on this checklist. The practices included in the checklist below are discussed at some length in the training courses. Please see http://www.linuxfoundation.org/programs/legal/compliance/training-and-education for course descriptions. Those companies further down the road can use the checklist to gauge their progress in implementing an effective compliance process and guide them in setting process improvement priorities. Where the checklist highlights the need for additional work, organizations will benefit from training, benchmarking, and communicating with other companies about approaches to specific practices that have been demonstrated to be effective. The Open Compliance Program stands ready and able to assist in these endeavors.

The self-assessment checklist presents a set of recommended practices distilled from the experiences of corporations committed to encouraging open source use while fully complying with OSS license obligations. Not every organization will see a need to implement every practice and some will find alternative practices or implementation approaches that achieve the goals of a compliance program. Appropriately, an organization will adapt its compliance approach based upon the nature and amount of the open source it uses, the licenses that apply to open source it uses, the kinds of products it distributes, and the design of the product itself.

How to Use the Checklist

The Self-Assessment Checklist can be used to stimulate discussion about the rigor and effectiveness of a compliance program and to focus attention on areas of greatest need for improvement. A facilitated discussion of checklist questions may be fruitful in achieving a consensus view of capability and gaining perspective on improvement possibilities.

The checklist may also be used by organizations, especially during the supplier selection process, to assess a supplier's compliance process and gauge the likely reliability of its open source disclosures.

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

No scoring scheme has been provided in this initial version of the checklist. Organizations may wish to consider the following approaches to appraising individual compliance practices:

- Yes / No / Not Applicable
- Frequently Performed / Occasionally Performed / Rarely Performed
- Strong / Satisfactory / Weak / Not Done
- Fully Satisfied / Partly Satisfied / Not Satisfied
- Green (Good) / Yellow (Marginal) / Red (Unacceptable)

Organizations may also wish to consider ways of aggregating the appraisal of individual practices into a composite view of compliance capability. For instance, satisfaction of supporting practices may be used to assess whether the goals of core compliance processes (Discovery, Review and Approval, Obligation Satisfaction, and Community Contributions) have been satisfied (in the mode of the Software Engineering Institute's Capability Maturity Model). Alternatively (as with ISO 9000 certification appraisals), major and minor "deviations" may be noted in a summary report. (In ISO 9000 terminology, minor deviations or nonconformities, though significant and requiring corrective actions, could be numerous but still not present a certification obstacle. However, a major deviation – even a single one – could be fatal to certification.)

As with the Software Engineering Institute's appraisal program, checklist users should distinguish between a practice that exists as a paper definition from one that is routinely used and relied upon to achieve compliance. Think of this as "institutionalizing" a practice, in other words becoming "the way you do business." In the original SEI training, appraisers were taught to assess the following common features to determine whether an organization had met its capability goals:

- Commitment to perform (as evidenced by policy and documented process requirements)
- Ability to perform (availability of skilled staffing, resources, and funding)
- Activities (the key practices used)
- Measurement and analysis (measures and metrics used to monitor process execution)
- Verification (audits and assessments used to confirm the right things were done)

In using the Self-Assessment Checklist, organizations can apply a similar line of analysis to determine whether an effective open compliance program has been established.

Feedback and Future Revisions

Suggestions for improvement of the Self-Assessment Checklist will be appreciated, in addition to feedback on the manner in which organizations are using the checklist. Please send comments to compliance@linuxfoundation.org. Feedback provided to the Linux Foundation will not be attributed to the provider to encourage organizations to share their thoughts on compliance and on the uses they are making of the checklist.

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

Additional Readings and Resources

The Linux Foundation has created three training courses on open compliance:

- **LF281 Executive Review of Open Source Compliance.** Half-day training, for executive management, focusing on the importance of compliance and what must be done to satisfy open source license obligations.
- **LF384 Overview of Open Source Compliance End-to-End Process.** A one-day comprehensive review of the compliance process, covering what must be done and recommending approaches to instantiating a compliance process.
- **LF488 Implementation and Management of Open Source Compliance.** A two-day comprehensive coverage of the compliance process, including working sessions with the compliance team on how to adapt compliance activities to the organization's needs.

The Linux Foundation has also published a number of white papers on compliance, available at http://www.linuxfoundation.org/programs/legal/compliance/training-and-education, including

- "Free and Open Source Software Compliance: The Basics You Must Know"
- "Establishing Free and Open Source Software Compliance Programs: Challenges and Solutions"
- "Free and Open Source Software Compliance: Who Does What"
- "Managing FOSS Compliance in the Enterprise"
- "FOSS Compliance: A Glimpse into Operational Best Known Practices"

In addition, the Linux Foundation has created a number of tools to assist companies in their due diligence activities. These tools are available for download at http://www.linuxfoundation.org/programs/legal/compliance/tools and are described in the following white papers, available for download at the same URL:

- "Dependency Checker Tool: Overview and Discussion"
- "Code Janitor Tool: Overview and Discussion"

Acronyms

FMEA	Failure Mode Effects Analysis
IT	Information Technology
OSRB	Open Source Review Board
OSS	Open Source Software

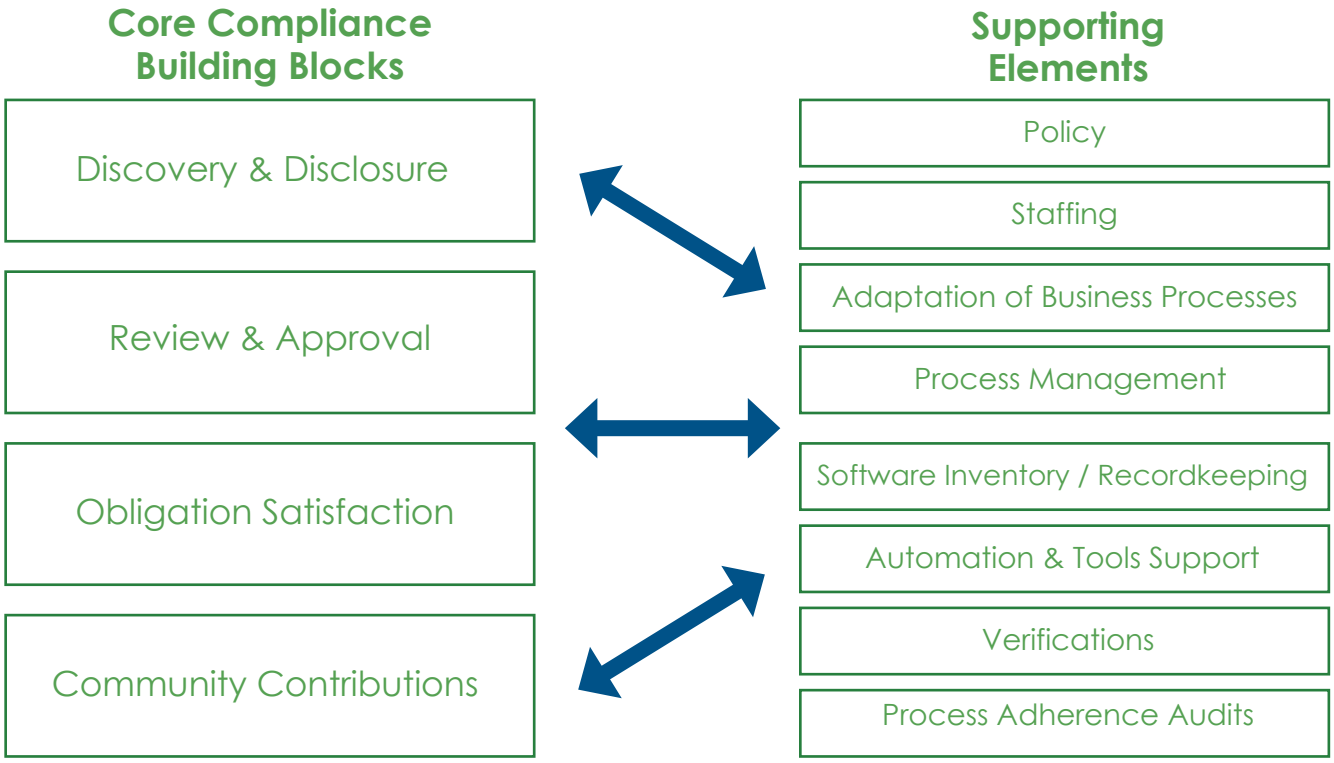
OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

Introduction

The practices that follow are organized and presented according to the notion of core compliance processes and supporting elements, as illustrated below. (The core processes are presented first, top to bottom, then the supporting elements, top to bottom.) The supporting elements are practices that enable an organization to accomplish the goals and objectives of the core compliance processes.



OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

Discovery

Discovery concerns itself with identifying the third party licensed software, including open source software, in a product readied for release. Key practices and capabilities in this area include the following:

Notes:

1. OSS discovery occurs at an early point in the product development cycle. ☐
2. The product team systematically identifies all the software and additional materials that must be subjected to compliance analysis. ☐
3. Third party suppliers disclose all OSS in their deliverables. ☐
   a) A defined format for the disclosure is used.
   b) The OSS compliance team reviews the disclosure for accuracy and completeness using whatever tools are available to it.
4. The organization investigates the third party supplier's use of OSS and its OSS compliance practices as part of its supplier selection process. ☐
   a) The organization investigates the third party supplier's compliance and supply chain management practices to evaluate their adequacy.
   b) The organization uses defined guidelines to determine if automated scanning or other confirmation of the supplier's disclosure is needed.
   c) Software license agreements include appropriate terms and conditions concerning OSS.
   d) 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
5. The organization periodically conducts audits of OSS use. ☐
   a) At an agreed-upon frequency, the organization conducts an audit/inventory of OSS used internally and records its findings.
   b) The organization audits and inventories the OSS included in its products for distribution.
   c) The organization identifies the conditions or events that trigger a fresh audit of the product's source code or of the incremental changes to a code base whose OSS compliance had previously been verified.
6. A bill of materials is prepared to reflect the open source content of a specific product release. ☐
   a) Code scans are used to prepare the bill of materials wherever source code is available.
   b) Supplier disclosures are used in cases where source code is not available.
7. The organization devises a systematic approach to identifying changes in the code baseline and performing incremental compliance on changes in an efficient manner. ☐
8. The organization systematically achieves closure on issues arising from discovery activity. ☐
   a) The organization systematically tracks open issues.
   b) The organization assigns adequate resources to achieve closure in a reasonable timeframe.
9. The organization periodically reviews commercial and open source tools to assess the costs and benefits of their use in discovering OSS in code baselines. ☐

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

Review and Approval

Review and Approval reviews the planned use of open source in products for distribution and, if mandated by company policy, in internal projects.

Notes:

1. The organization subjects all open source use in products to review and defines what contextual changes in OSS use trigger re-approval activity. ☐
2. The organization considers issues relevant to the use of a specific OSS package and version, e.g. bug fixes the community has made in subsequent versions, security vulnerabilities that have been identified in a specific package version, technology incorporated into the package that might be subject to export control regulations, etc. ☐
3. An open source review board is used to review and approve planned uses of OSS in products for distribution. ☐
   a)The OSRB is staffed with appropriately skilled and knowledgeable individuals.
   b)Appropriate resources are available for the interpretation of OSS licenses and definition of obligations to be satisfied.
   c)Sufficient staffing is provided to the OSRB to achieve turnaround time on submissions that supports product development cycles.
   d)OSRB procedures (inputs to a review, participants, review procedures, analysis procedures, decision outcomes, appeal and waiver procedures, etc.) are defined and documented.
   e)The OSRB considers and provides architectural guidelines and/or requirements for OSS inclusion in products to be distributed.
   f)The OSRB uses independent analysis methods to confirm the OSS content reported by teams when they submit an OSS use case for approval.
   g)Records of OSRB deliberations are maintained (cases, status, past decisions, requirements imposed on product teams, etc.) and used in future deliberations.
   h)The OSRB decides whether to approve the proposed OSS use and identifies obligations that must be satisfied, if any, and conditions that must be met, if any, before product distribution is approved.
4. The organization provides a definition and examples of the information that must be submitted to the OSRB for approval of OSS use. ☐
   a) Proposed use of OSS includes a description of the architectural interfaces and dependencies between any OSS components and the rest of the system.
5. The OSRB communicates perspectives across business units to achieve a consistency of interpretation of license obligations and review practices. ☐

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

Obligation Satisfaction

Obligation Satisfaction covers compliance practices needed to satisfy OSS license obligations

Notes:

1. The organization assures that its third party suppliers provide all information that is necessary to satisfy OSS obligations when the product is distributed, e.g. copyright notices and attributions, license text, corresponding source code that must be made available, etc. ☐
2. The organization defines what modes of external software conveyance trigger license obligations and assures that any software thus released meets compliance requirements. ☐
3. The organization satisfies obligations in a consistent and disciplined manner. ☐
   a)The organization makes available a repository of license texts and obligation requirements to assure consistent interpretation and compliance activities.
   b)The organization provides explicit examples of ways to satisfy obligations.
   c)Skilled and knowledgeable individuals write the OSS-relevant sections of product documentation and satisfy the other license obligations that must be met.
4. The organization places into a software repository the complete source code corresponding exactly to each OSS package used in a given product release. ☐
   a)Teams provide, as required by specific licenses, the complete source code, which may include any associated interface definition files, plus the scripts used to control compilation and installation of the executable.
   b)Verification activities are used to assure that corresponding source code for the OSS can be built outside the organization's build environment and that the resultant binaries for the OSS packages match the product binaries.
   c)Verification activities assure that source code to be distributed has been cleansed of any inappropriate comments.
   d)Verification activities assure that all OSS packages to be distributed have been approved by the OSRB.
5. Source code reviews are used during the development phase to assure that OSS packages contain necessary and appropriate documentation of copyright, attribution, licensing, and change log information. ☐
6. Activities to assess and satisfy OSS license obligations are planned and integrated into project schedules to assure that obligations are met in time for product release. ☐
7. A defined code distribution mechanism is used to respond to routine requests for source code distribution. ☐
   a)The organization defines a code distribution mechanism that satisfies the requirements of particular OSS licenses.
   b)A web portal or other face to the community is created to provide online access to source code used in company products.
   c)Responsibility for operating the portal is assigned and staffed appropriately.

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

Notes:

d) Procedures are established to assure that correct and complete versions of OSS are posted.
e) The portal is organized in a clear and meaningful way to provide users easy access to products' licensing information and, if appropriate, source code.

8. Individuals or teams responsible for documentation and localization activities perform necessary tasks to assure that obligations are met. ☐
a) Support teams (e.g. supply chain, documentation, IT) are trained in OSS fundamentals.
b) Involvement of support functions is planned, scheduled, and performed in a timely manner.

9. The organization responds to all external compliance requests in a timely manner. ☐
a) A compliance fulfillment process exists for satisfying routine requests.
b) Metrics are routinely collected and reported on response time.
c) A compliance inquiry response process exists.
   i) Response actions are given high priority and issues are escalated to an appropriate level of management.
   ii) Appropriate oversight, review, and approval of compliance actions is provided.
   iii) Modifications to the organization's defined compliance process are made as appropriate to prevent recurrence of compliance issues.
d) Compliance requests are tracked to closure.
e) If determined to be necessary, efforts to re-write copyrighted code as proprietary software under cleanroom conditions are carried out according to a defined procedure.

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

Community Contributions

Community Contributions concerns itself with the review and approval of employee contributions to community projects, as well as company contributions of code and other resources to community projects.

Notes:

1. Community contributions are reviewed and approved according to a defined process. ☐
2. A determination is made whether an employee's proposed contribution is work-related or non-work-related based upon an existing guideline. ☐
   a)The consequent scope of review and approval authority is determined.
3. Community contributor license agreements are reviewed by the OSRB and the company's law department. ☐
4. A mechanism is used to determine whether any of the organization's business units object to the proposed contribution. ☐
5. Copyright ownership of the planned contribution is clarified. ☐
6. A mechanism is used to initiate and plan company contributions of financial support, labor, code, or other intellectual property to community projects. ☐
7. Company contributions to open source communities are tracked (e.g. both individual contributions such as bug fixes as well as company-sponsored projects). ☐

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

Policy

The Policy area addresses corporate policy to encourage use of OSS at the same time protecting the company's business interests.

Notes:

1. An organizational policy enables the company to incorporate and use OSS in their products. The policy is signed by a senior executive and is communicated to the entire workforce. ☐
2. At a minimum, the policy addresses roles and responsibilities for compliance actions, a review and approval process for use of OSS, guidelines for contributions to community projects and a review and approval process for contributions, and core processes that must be implemented to govern use of OSS in company products. ☐
3. The management team endorses the policy and assures that all employees involved with open source understand and follow the policy. ☐

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

Adequate Compliance Staffing

Adequate Compliance Staffing focuses on the skilled resources needed to implement the compliance program.

Notes:

1. Skilled and knowledgeable individuals are made available to contribute to the compliance effort. ☐
2. Dedicated assignments to the compliance function provide continuity of involvement and accumulation of expertise. ☐
3. Job descriptions identify the skills and insights needed to perform compliance functions adequately. ☐
4. The organization identifies individuals with the skills, insights, and interest needed to contribute to the compliance function. ☐
5. Compliance contributors are drawn from cross-functional departments, as needed. ☐
6. Training and experiential learning opportunities are provided to build necessary skillsets. ☐
   a) Individuals performing compliance functions in different business units are encouraged to communicate and share expertise and perspectives amongst themselves to achieve a consistent compliance approach.
7. External consultants are hired, as needed, to augment the internal compliance effort. ☐
8. Estimates of total compliance effort and duration are prepared to address the organization's compliance requirements. ☐
9. Estimates of one-time and overhead activities are estimated and tracked ☐
10. Estimates of product-related compliance activities are estimated and tracked from the perspective of both the organizational compliance team and the product team. ☐
11. A staffing plan is prepared and followed to provide a level of responsiveness and cycle time adequate for product release cycles. ☐
12. Progress is tracked against the organization's and product team's compliance plans and additional resources are added as needed to achieve compliance objectives. ☐

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

Adaptation of Business Processes

Adaptation of Business Processes focuses on fitting OSS compliance concerns within the context of existing business processes.

Notes:

1. Existing business processes are modified to incorporate OSS compliance activities and considerations. ☐
   a) Compliance activities are mapped against the organization's product development process to identify leverage points.
   b) A process FMEA (failure mode effects analysis) is performed to identify ways that compliance failures could occur and the business processes that should be modified to prevent such failures.
2. Supply Chain's supplier selection procedures are tailored to assure that OSS compliance requirements are considered when performing due diligence on suppliers. ☐
3. Process management assures that OSS compliance activities are included early enough in the product development cycle to enable the organization to meet its release timelines. ☐
4. Late-cycle verification steps are used to assure that all compliance requirements have been met before external distribution occurs. ☐
5. Individuals charged with managing business processes have received training in OSS compliance requirements and exhibit sensitivity to OSS compliance concerns. ☐

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

Training

Training addresses the communications needed to assure that the entire company understands what must be done to achieve OSS compliance.

Notes:

1. Basic training on the organization's OSS policy and on the benefits of OSS use is provided to all who come into contact with OSS or are involved in customer and supplier interactions and in product distribution activities. ☐
   a) The organization maintains a definition of who must take training.
   b) Training records are maintained.
      i) Training objectives are set.
      ii) Follow-up actions are taken to assure planned training is completed.
   c) OSS training is integrated into the organization's training curriculum and made a part of organizational and personal objectives.
   d) OSS training is provided as part of new hire orientation.
2. Additional training on OSS-related topics is provided to augment the basic curriculum for both managers and non-managers. Examples include organizational procedures; tools; OSS licenses; software architectural guidelines; etc. ☐
3. Growth of an internal community of OSS users is encouraged in order to provide organizational guidance and leadership with respect to the use of OSS in an ethical and compliant way. ☐
4. Refresher training on OSS compliance is provided periodically. ☐

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

Compliance Process Management

Compliance Process Management focuses on establishing, maintaining, and improving a process capability to achieve OSS compliance.

Notes:

1. Overall responsibility for achieving organization-wide OSS compliance is clearly designated. ☐
   a) The designated compliance officer has access to the organization's senior executives to escalate compliance issues whenever needed.
   b) The compliance support team has access to functional specialties to guide or perform compliance activities, e.g. OSRB, documentation production, IT, etc.
   c) An individual or team is designated as the organization's point of contact to the external OSS community for compliance-related communications.
   d) An ombudsman is established so that individual employees have a channel of communication to voice their concerns or questions.
2. The team responsible for coordinating compliance activities has visibility into product development and product release plans and activities, and is able to interface effectively with product teams. ☐
3. Project management fundamentals are applied to managing compliance projects and compliance team activities. ☐
   a) Compliance goals and objectives are set.
   b) Compliance project priorities are set.
   c) Compliance effort is estimated.
   d) Compliance resources are assigned.
   e) Compliance projects are planned and scheduled, progress is tracked, and issues are escalated as needed.
4. Metrics are defined and collected to assess the effectiveness of the organization's OSS use and its OSS compliance activities. ☐
   a) Corrective actions are taken to address process inadequacies.
   b) A process improvement plan is established for the compliance process.
5. The organization engages in externally-focused benchmarking activities to identify potential improvements to its compliance process. ☐
6. The organization maintains an awareness of community initiatives to address supply chain issues with respect to OSS compliance. ☐

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

OSS Inventory / Recordkeeping

OSS Inventory / Recordkeeping addresses the organization's need to maintain accurate records of OSS content and OSS compliance activities to support responses to compliance inquiries and changes in the compliance environment.

Notes:

1. The organization tracks progress of compliance activities for a product being readied for release. ☐
   a)The organization tracks progress of the OSS discovery process and of scans and audits on the product's code.
   b)The organization systematically tracks closure of OSS issues identified during the discovery process.
   c)The organization tracks progress of the review and approval process for OSS cases.
   d)The organization tracks progress of obligation satisfaction for a product being readied for release.
2. The organization maintains complete and accurate records about the OSS content in its products, and the context in which it is used, according to a defined procedure. ☐
   a)A defined format is used to record information about the OSS included.
   b)The OSRB maintains accurate records about its reviews and review outcomes, including any limitations or conditions on approval that might necessitate a different outcome in another context.
   c)The organization uses past records of OSS review and approval as an aid when reviewing new OSS cases for approval.
3. The organization maintains complete and accurate records about OSS used internally for tools, operational systems, prototype development, etc. ☐
   a)The organization reviews records of OSS internal use periodically to identify opportunities to save money, improve performance, and achieve operational synergies.

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

Automation / Tool Support

Automation / Tool Support examines the organization's use and consideration of tools to support its compliance activities.

Notes:

1. The organization assesses its compliance process to identify and prioritize opportunities for automation and tool support. ☐
2. The organization regularly investigates commercial and OSS tools that might provide assistance to compliance activities. ☐
   a) A systematic approach to tool evaluation is taken.
      i) Tool requirements are documented.
      ii) A tool evaluation plan is established and executed.
      iii) Use cases and pilot projects are defined.
      iv) Evaluation licenses are acquired or other mechanisms for experimenting with tools are used.
3. Tool acquisition or tool development projects are planned and executed according to defined procedures for tool development and adoption. ☐
4. The organization engages in user group meetings and community forums related to compliance tools. ☐
5. Mechanisms are used to determine the OSS content of a product release and the files that must be subjected to compliance analysis. ☐
6. Tools are used to track OSS issues to closure. ☐
7. Mechanisms are used to determine the differences in software content between individual releases of a product for distribution. ☐
8. An initial compliance baseline for a product is established with the aid of scanning tools, whenever it is advantageous to do so. ☐
9. A repository of OSS packages is maintained and made available to the organization. ☐

OPEN COMPLIANCE PROGRAM
1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org
THE LINUX FOUNDATION

Verification

Verification concerns the independent assurance steps taken by the OSS compliance team to confirm that OSS obligations have been properly met.

Notes:

1. The compliance team performs verification activities according to a defined procedure. ☐
2. The compliance team verifies that source code license obligations have been met by the time a product is considered ready for release. ☐
   a)The compliance team verifies that any offers of source code have been included as required.
   b)The compliance team verifies that source code is placed in a distribution staging area for each OSS package included in a product readied for release and that a satisfactory distribution mechanism exists for any source code that must be made available.
   c)The compliance team verifies that source code to be made available corresponds exactly to the binaries in the product.
   d)The compliance team verifies that source code can be built outside the organization's build environment.
3. The compliance team verifies that copyright notices, attribution notices, license text, and any modification logs have been included accurately. ☐
4. The compliance team verifies that OSRB approval has been obtained for all OSS packages in the release. ☐
5. The compliance team verifies that third party suppliers have made full and accurate disclosure of open source included in their deliverables and that these suppliers have satisfied their obligations under the OSS licenses. ☐
6. The compliance team verifies that open source can be obtained via the defined distribution mechanism and that the source code thus obtained can be built in an independent environment. ☐

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

Process Adherence Audits

Process Adherence Audits refer to the checks the organization performs to determine whether it is using its defined compliance process and obtaining expected results from its use.

Notes:

1. Process adherence audits are used to determine whether the organization follows its defined compliance process. ☐
   a) Audits identify the instances in which non-standard reviews were used.
2. Audits assess the extent to which execution of the compliance process produces expected compliance results. ☐
3. Audits determine whether the organization maintains accurate records about the OSS content of its products and of the compliance activities it performs. ☐

--- END OF CHECKLIST ---

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

About the Open Compliance Program

The Linux Foundation's Open Compliance Program is the industry's only neutral, comprehensive software compliance initiative. By marshaling the resources of its members and leaders in the compliance community, the Linux Foundation brings together the individuals, companies and legal entities needed to expand the use of open source software while decreasing legal costs and FUD. The Open Compliance Program offers comprehensive training and informational materials, open source tools, an online community (FOSSBazaar), a best practices checklist, a rapid alert directory of company's compliance officers and a standard to help companies uniformly tag and report software used in their products. The Open Compliance Program is led by experts in the compliance industry and backed by such organizations as the Adobe, AMD, ARM Limited, Cisco Systems, Google, HP, IBM, Intel, Motorola, NEC, Novell, Samsung, Software Freedom Law Center, Sony Electronics and many more. More information can be found at http://www.linuxfoundation.org/programs/legal/compliance.

OPEN COMPLIANCE PROGRAM

1796 18th Street, Suite C
San Francisco, CA 94107
+1 415 723 9709
http://www.linuxfoundation.org
compliance@linuxfoundation.org

THE LINUX FOUNDATION

The Linux Foundation promotes, protects and advances Linux by providing unified resources and services needed for open source to successfully compete with closed platforms.

To learn more about The Linux Foundation, the Open Compliance Program or our other initiatives please visit us at http://www.linuxfoundation.org/.