Professional Open Source Software Management Assessment Results

Produced for Client by LF Consulting

Table of Contents

Overview

The proliferation of open source software (OSS) has escalated in the last five years to the extent that it is now pervasive. Gartner reports that 85% of organizations use open source, and 87% of users say open source meets or exceeded their expectations.

There are many reasons for using OSS that are often compelling:

- The best-in-class software in some areas is OSS
- Product must interoperate with other OSS, e.g. Linux
- Customers favor or even require OSS
- Faster time to market by avoiding development and testing of new code
- Provides a lower cost alternative to traditional commercial packages
- Need for software that can be modifed or customized to specific applications
- Lower development costs by using free, already de-bugged code
- Lower code maintenance costs by taking advantage of community maintenance
- OSS accompanied a corporate acquisition
- Code-base already contains significant OSS

While the use of OSS offers many important advantages, it also creates significant new management challenges. However, Gartner also reports that fewer than 40% of organizations have an open source policy and even fewer have tools and controls for managing it or ensuring compliance with its licenses. Companies that do not have an effective open source management program covering multiple dimensions of management will not fully leverage open source software and will face unnecessary risks due to unknown license issues, support issues, security vulnerabilities and export restrictions. Some specific management challenges are:

- Handling a much higher volume of code acquisition decisions
- Maintaining code and version consistency across an organization
- Insuring license compliance at distribution or deployment time
- Managing support for many external elements
- Managing participation in public communities

All of these challenges have been addressed by the leaders in OSS adoption. Their “best practices” have been proven to effectively manage the complexity and risk associated with OSS while enhancing the development productivity and delivering a good return on the investment in the management program itself. The purpose of this assessment is to help you and your company become aware of these best practices for OSS management and to measure where your organization stands in its use of these techniques.

Open Source Management Assessment

The Open Source Management Assessment service evaluates an organization's approach to managing its use of open source across eight key dimensions:

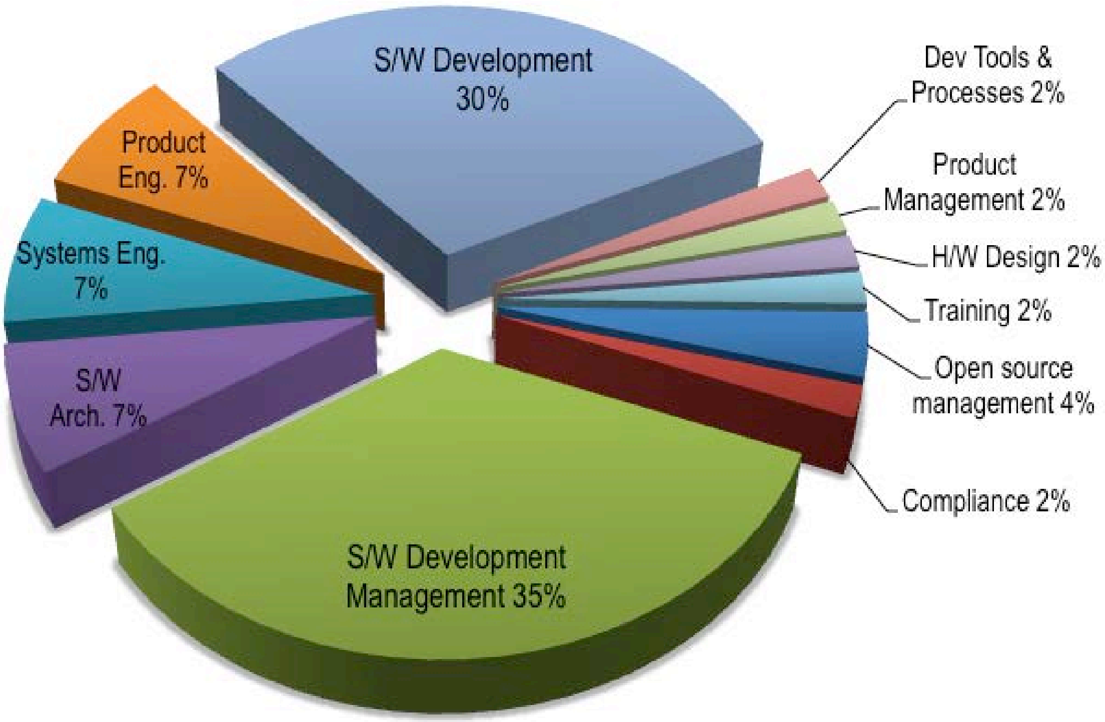
1. **Open Source Discovery**
   How do developers in your organization go about finding OSS for inclusion in their projects?
2. **Open Source Review and Selection**
   How does your organization evaluate and approve OSS components for inclusion in your software base?
3. **Open Source Supply Chain Management**
   How does your organization monitor and control Open Source Software components introduced into your company via your software supply chain?
4. **Open Source Code Management**
   How does your organization keep track of and manage open source code components that have been included in your software base?
5. **Open Source Maintenance and Support**
   How does your organization maintain the OS components that have been included in your software base, and how do your engineers get technical support for these components?
6. **Open Source Compliance Program**
   How does your organization make sure that your company is in compliance with the licenses of open source components that have been included in your software base?
7. **Open Source Community Interaction**
   How does your organization interact with the OS communities that produce the components that have been included in your software base or that are closely aligned with your target markets?
8. **Executive Oversight**
   How do line-of-business management, engineering management and corporate counsel participate in the management of open source software to provide appropriate oversight?

Upon receipt of the completed surveys, LF Consulting has analyzed the results and assigned a maturity level to each dimension. These maturity levels indicate how your organization's practices compare with software industry best practices in the use of open source software.

1. **Exposed**
   One or more essential elements of open source software management are not addressed by current practices causing the company to be exposed to unnecessary risk.
2. **Measured**
   Essential information exists but adequate risk management depends on individuals and manual or undocumented processes.
3. **Managing**
   An adequate framework for management of open source software and its risks is in place, however community resources are not well leveraged.
4. **Participating**
   Management processes are in place to leverage the technical resources of the OS communities allowing company to achieve higher levels of product quality and supportability at lower cost. Processes are automated where appropriate and supported by tooling.
5. **Driving**
   The company exercises leadership in relevant open source communities in order to drive its technical and strategic objectives. Full benefit is realized from open source software and communities.

Survey Demographics

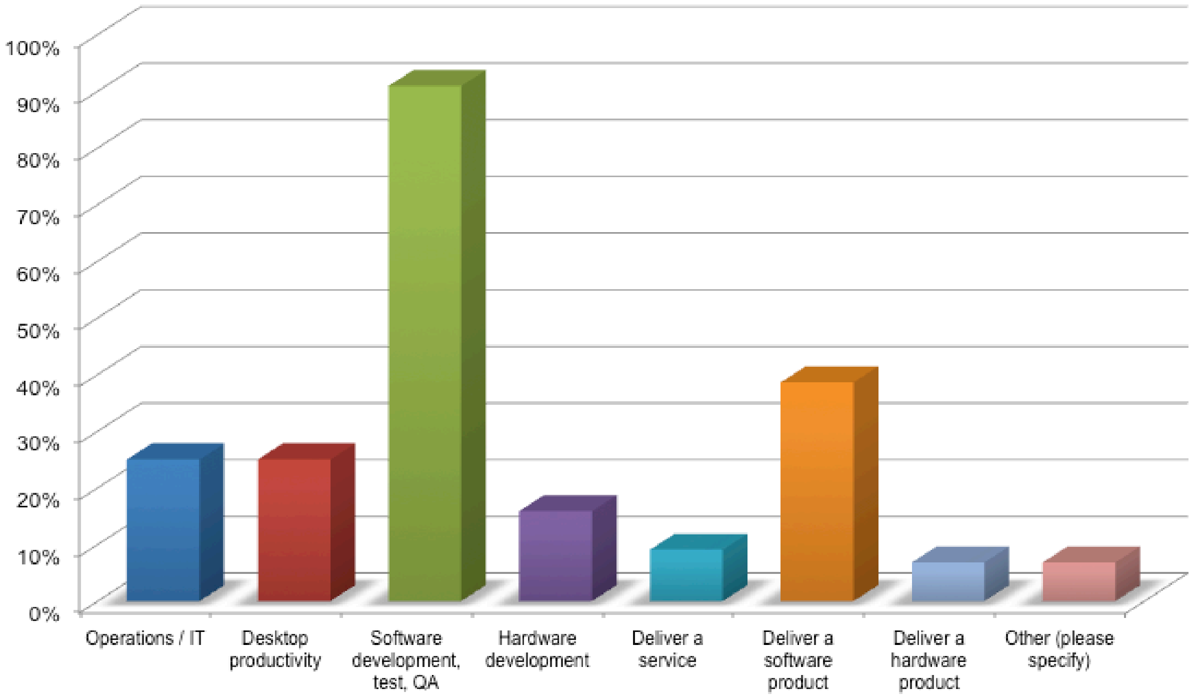
Respondent Demographics



It is notable and problematic that there were no respondents from QA, Legal or Supply Chain management.

Where is OSS Used / Deployed at CLIENT?

To the best of their knowledge, respondents indicated that OSS is used and deployed in the following areas:



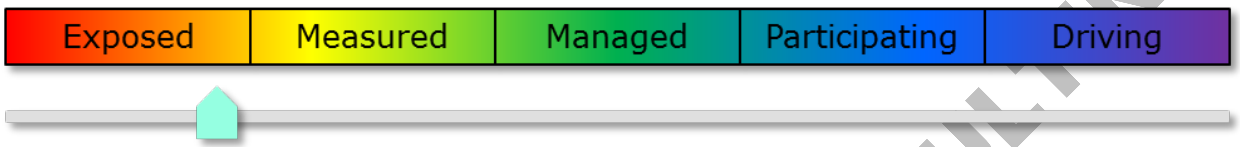
The “Other” areas stated include system integration, SCM, Bug Tracking, and SW Project Management

Assessment Results

LF Consulting has analyzed the respondents provided to our survey and developed the following conclusions in each dimension of open source software management:

Open Source Discovery

How do developers in your organization go about finding open source software for inclusion in their projects?



Current Practices:

- The majority of respondents (63%) indicated that CLIENT does not provide formal or written guidelines to developers on where to find third party software including open source software (or that they did not know of any guidelines).
- A minority of respondents (< 15%) indicated that some guidelines do exist or that each department had its own guidelines.
- No respondents indicated tools are used in house at CLIENT to search for already existing and approved open source in your enterprise.

Potential Risks:

- Engineers are likely to waste time by searching for applicable open source and evaluating OSS components that should not be approved for use.
- Component and version proliferation may occur, leading to increased complexity, security and support cost.
- Lack of tooling makes it hard to leverage information from others in the organization, leading to duplication of efforts.
- Lack of communicated policy gives rise to variance in practices among departments, resulting in inefficiencies and potential conflicts in practices across CLIENT

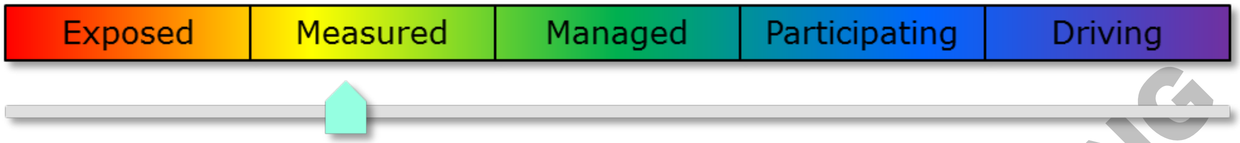
Comparison with Earler POSMA

The assessment for Open Source Discovery is unchanged from the value of 2 years ago.

Maturity Level - **Exposed**

Open Source Review and Selection

How does your organization evaluate and approve open source software for inclusion in your software base?



Current Practices:

- With regard to selecting third party code including commercial and open source, CLIENT engineers decide individually what components to use without approvals, or teams create their own guidelines. This is the prevailing practice with OSS code downloaded from the Internet (97%) and also for commercial OSS (61%) and proprietary commercial software (56%)
- Department managers and development tools departments have some role in reviewing third party component selection and encouraging reuse of known successful components, primarily withinput on commercial open source (91%)
- One third of respondents indicated that guidelines exist to review OSS in a standard manner.
- A very small number of respondents (7%) indicated that a review board existed for commercial open source and for proprietary third-party software, but not for OSS acquired from the Internet.

Potential Risks:

- For OSS incorporated in your projects that is subsequently redistributed to customers, not having formal processes and review boards can expose CLIENT to the risk of incorporating OSS that is not appropriate for intended use or legal compliance requirements.
- Lack of tooling in use make it difficult to handle third party software requests, approvals and record keeping in a timely manner. This can impact product release schedules, delay innovation and encourage non-compliance.

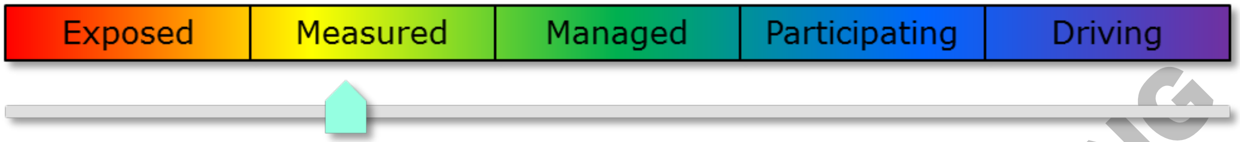
Comparison with Earlier OSMA

The assessment for Open Source Review and Selection is slightly improved from the value of 2 years ago, in that more respondents indicated that they believed there to be formal processes for review and selection.

Maturity Level - **Measured**

Open Source Supply Chain Management

How does your organization monitor and control open source software components introduced into your company via your software supply chain?



Current Practices:

- Respondents were divided as to whether CLIENT had specific requirements for suppliers regarding open source content (multiple responses allowed)
    - 33% indicated that no supplier requirements existed
    - 25% indicated that CLIENT requires suppliers to report OSS content and/or to warranty the accuracy of their reporting
    - 35% indicated that CLIENT itself verifies compatibility of supplier code with software in use at the company
    - 31% believed that CLIENT either requires that suppliers scan their own code and/or provide the text of licenses for code in their bills of material
    - Half of all respondents, however, were unsure as to any of the above requirements and practices

Potential Risks:

- Not having a formal process to validate OSS components from s/w vendors can lead CLIENT to incorporate undesired open source in project/product deliveries to customers and increase operational costs.
- Not reviewing vendor compliance programs does not encourage them to follow best practices and provides no basis upon which to judge the validity of OSS disclosures.
- Having no formal supply chain process can lead to risk of non-compliance to OSS licenses in vendor supplied code or cause issues for your partners who redistribute your software.
- Lack of communicated policy gives rise to variance in practices among vendors and acquisition group, resulting in inefficiencies and potential conflicts in practices across CLIENT

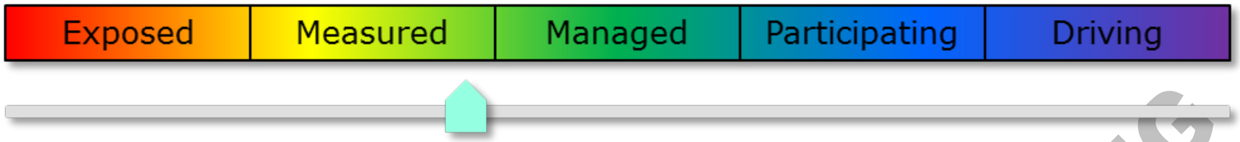
Comparison with Earlier POSMA

The assessment for Open Source Supply Chain Management is slightly improved from the value of 2 years ago, in that fewer respondents indicated that they believed there to be no formal supplier requirements.

Maturity Level - **Measured**

Open Source Code Management

How does your organization keep track of and manage open source code components that have been included in your software base?



Current Practices:

- Most respondents (75%) indicated that OSS components are treated in the same manner as third party commercial components, however they are tracked separately.
- Responses regarding the details of actual code management were mostly unknown, with few known practices for managing snippets, component ownership, automation, etc.
- CLIENT lacks a clear code management policy with defined governance processes and tools.

Potential Risks:

- Lack of formal central component location that is consistently used by the organization could lead to component & version proliferation.
- No formal tracking procedures at the release or usage level can lead to errors in component inventories.
- Lack of tooling supporting an automated process is inefficient and provides no validation of against policies and make it very difficult to track OSS inserted directly into the code base (as opposed to full OSS components that can be tracked by Configuration Management via build dependencies.

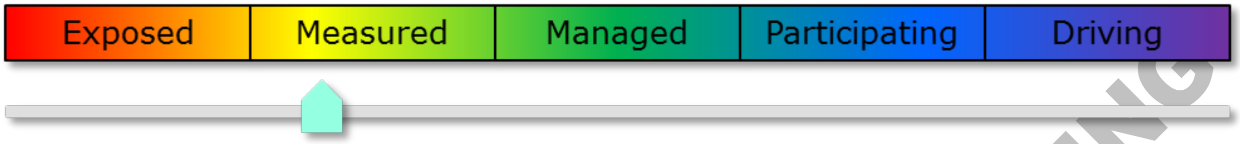
Comparison with Earlier POSMA

The assessment for Open Source Code Management is slightly improved from the value of 2 years ago, in that a few more respondents indicated that they believed that CLIENT segregated OSS components in a separate repository and/or reviews and tracks use of OSS components across applications.

Maturity Level - **Measured**

Open Source Maintenance and Support

How does your organization maintain the open source components that have been included in your software base, and how do your developers and support engineers get technical support for these components?



Current Practices:

- The vast majority of respondents indicated that no formal maintenance or support responsibilities exist. Developers who deploy OSS do as they see fit with regards to OSS maintenance & support without guidance.
- A reasonable cohort (22%) indicated that once software is deployed, CLIENT performs no further maintenance
- A small number of respondents (13%) indicated that formal component ownership policy and tracking process exists.
- A minority (<10%) reported that automated processes exist to track issues, fixes, versions and compatibility requirements
- A support strategy is not considered for the OSS components when they are introduced and no approach to reduce cost of support via consolidation is implemented.

Potential Risks:

- No formal support policies can lead to increased support costs or decreased issue resolution time. Lack of support policy can impact internal development efforts and customer service levels.
- Locally fixed bugs, vulnerabilities and enhancements must be re-patched for each new open source release. This practice slows adoption of OSS and increases maintenance costs.
- Duplicate activities may occur through the organization to resolve support and maintenance issues on commonly use OSS.
- Lack of automation or tools raises costs and reduces effectiveness for maintenance of OSS components

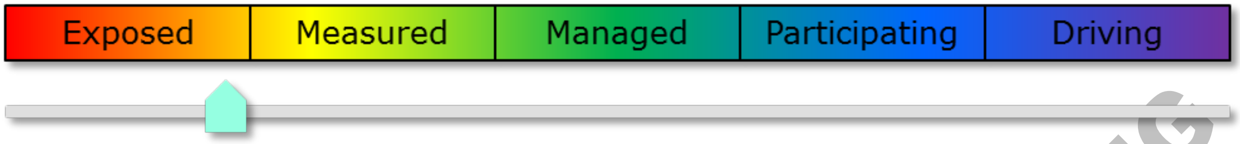
Comparison with Earlier POSMA

The assessment for Open Source Maintenance and Support is slightly improved from the value of 2 years ago, in that CLIENT establishes owner(s) for components and defines maintenance responsibilities and/or support responsibilities.

Maturity Level - **Measured**

Open Source Compliance Program

How does your organization make sure that your company is in compliance with the licenses of open source components that have been included in your software base?



Current Practices:

- Many respondents (40%) indicated that no formal process exists to insure compliance to OSS licenses, especially the OSS contained in distributions made to customers and other third parties.
- Lack of a formal audit process on projects/releases incorporating open source, and only full OSS components are tracked.
- Lack of an automated process for tracking and reporting compliance requirements.

Potential Risks:

- No automated audit process leads to the increased risk of undocumented OSS elements that have “slipped into” the project or release and/or infringing on licenses as obligations were missed.
- Not verifying compliance can lead to increase remediation costs, legal costs and risk.
- IP issues can result due to lack of compliance with OSS licenses.

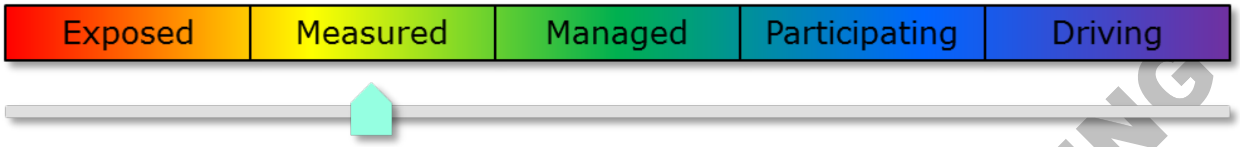
Comparison with Earlier POSMA

The assessment for Open Source Compliance is slightly improved from the value of 2 years ago, in that a fair number of respondents (37%) that CLIENT maintains a list of third party / open source components included in its software base and others (19%) claimed that CLIENT lists third party components in each release as part of release / roll-out process.

Maturity Level - **Exposed**

Open Source Community Interaction

How does your organization interact with the open source communities that produce the components that have been included in your software base or that are closely aligned with your target markets?



Current Practices:

- Beyond using OSS community code, there is some participation with OSS communities, yet it is ad-hoc and likely unmanaged.
- CLIENT developers do participate in OSS forums / bulletin boards / email list with company identification, however one respondent said this communication must be done without company identification.
- Bug fixes are not contributed back to the original OSS communities.
- One respondent indicated that direct communication and cooperation is actively performed with OSS community maintainers / committers for OSS you use.

Potential Risks:

- Not communicating with company identification can lead to reductions in community support and guidance on development of software that your company uses.
- Not contributing bug fixes can lead to maintenance productivity issues and can increase operational risk due to un-fixed bugs or sub-optimum usage.
- Not participating in OSS development creates the risk that important OSS projects might go in a direction that is not in accordance with your company strategy.
- By not participating in OSS communities, CLIENT will potentially be unattractive to developers who wish to participate in OSS development as a part of their employment and you will miss exposure to potential valuable future employees with needed OSS skills.

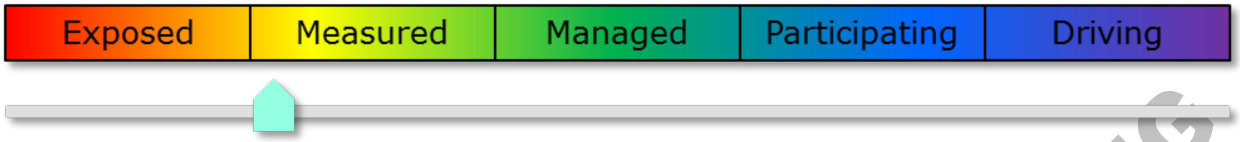
Comparison with Earlier POSMA

The assessment for Open Source Community Interaction is unchanged from the value of 2 years ago.

Maturity Level - **Measured**

Executive Oversight

How do line-of-business management, engineering management and corporate counsel participate in the management of open source software to provide appropriate oversight?



Current Practices:

- Executive participation is primarily through chain of command
- A small number of respondents (8%) indicated that CLIENT Legal must approve each open source license included in third party components for internal deployment
- Lack of any formalized involvement by key executive stakeholders in OSS review boards and overseeing OSS community involvement.
- Most respondents (63%) left this section blank on the survey forms.

Potential Risks

- The development and evolution of policy to optimize the way your business uses OSS is hindered. Executives may not make proper strategic decisions due to their lack of understanding of the value of OSS to the company.
- Lack of executive involvement can lead to increased operational and legal risk due to a lack of apparent oversight.

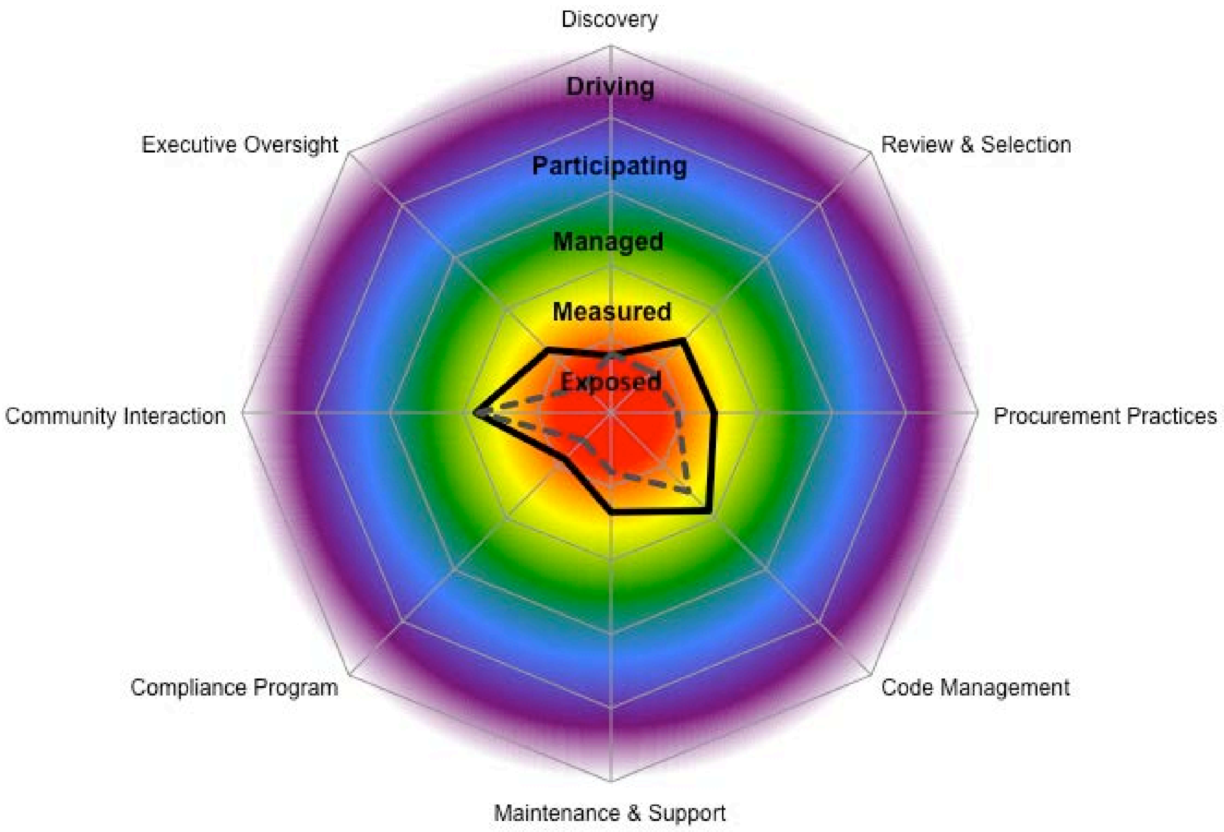
Comparison with Earlier POSMA

The assessment for Open Source Community Interaction is somewhat improved from the value of 2 years ago, in that more respondents indicated at least some involvement from the CLIENT legal department.

Maturity Level – **Measured**

Summary Results

The following radar chart shows each dimension of OSS management as a spoke in the chart with the length of each spoke indicating the maturity level for that particular dimension.



From the survey results, it is apparent that CLIENT has put some formal processes in place to manage the use of open source software. The black, solid-bordered polygon on the radar chart represents the level of OSS governance maturity from the practices in place today; the gray dotted region indicates the result of the POSMA of two years ago.

Based upon the survey results, LF would categorize CLIENT as a company still lacking a holistic open source governance program in which management of the open source is systemic in the overall operations of the company.

While there may be additional informal controls in place at CLIENT, IP and operational issues can arise due to undermanaged use of OSS. Many areas can see increased risk without an effective governance program in place.   Therefore, LF Consulting recommends that, at a minimum, companies should be at a “Managing” level across all disciplines in order to minimize both legal and operational risks of using OSS.

However, LF Consulting recommends that companies who want greater benefit from open source software should strive to reach the “Participating” level of maturity across all disciplines. Companies at the “Participating” level have implemented governance programs that are efficient, supported by tools, automated where possible, fully integrated into company operations, and look beyond the company boundaries and into the OSS communities and the extended supply chain. At this point, companies will achieve the full value of OSS.

The next section of this document includes a series of recommendations to help CLIENT achieve more with OSS. By implementing these recommendations, CLIENT will be fully at the Participating level of maturity across all disciplines.

Recommendations

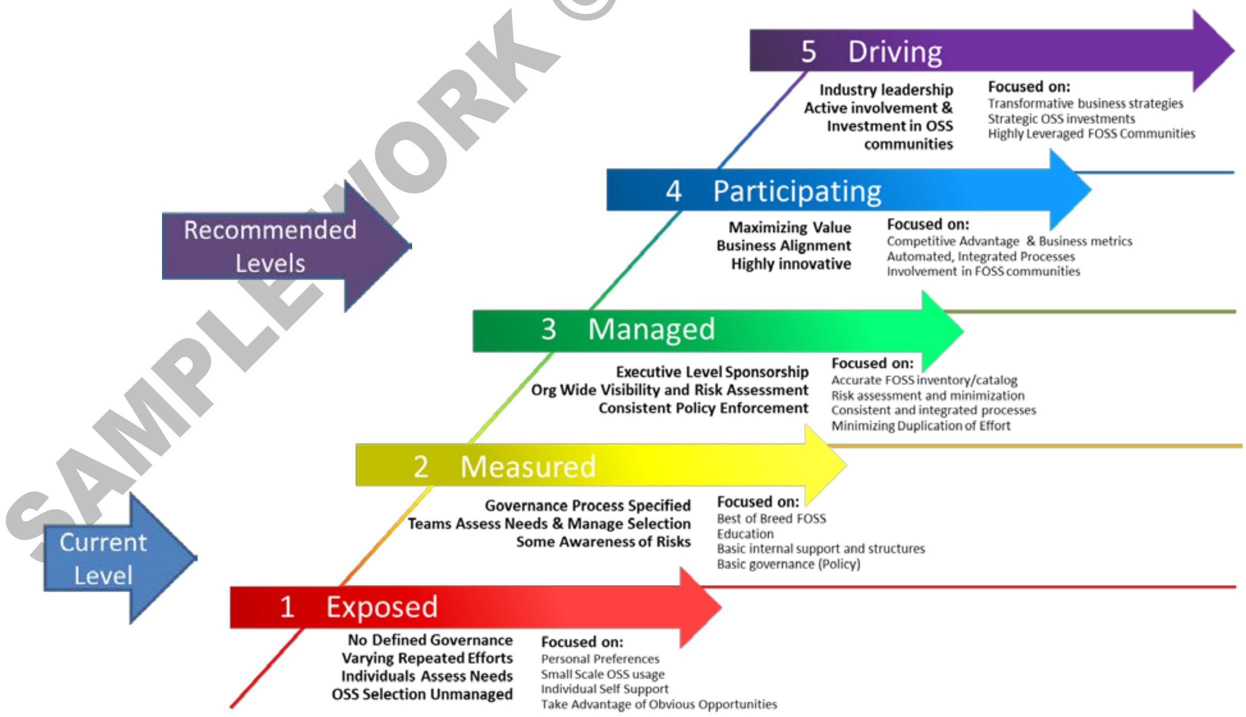
Based upon the survey results, LF Consulting suggests CLIENT consider the following recommendations. The recommendations are categorized in the following manner:

1) General Recommendations regarding the overall governance program
2) Specific recommendations in the different 8 areas of management

General Recommendations

According to the LF Consulting Open Source Maturity Model, CLIENT's overall maturity level toward open source governance is at the "Exposed" level. LF recommends that CLIENT consider making investments to

- Develop a top-down strategy for leveraging open source
- Improve open source governance
- Manage legal and operational risks associated with leveraging open source software
- Put a plan in place to enhance overall maturity level


5 Driving
Industry leadership
Active involvement & Investment in OSS communities
Focused on:
Transformative business strategies
Strategic OSS investments
Highly Leveraged FOSS Communities
4 Participating
Maximizing Value
Business Alignment
Highly innovative
Focused on:
Competitive Advantage & Business metrics
Automated, Integrated Processes
Involvement in FOSS communities
Recommended Levels
3 Managed
Executive Level Sponsorship
Org Wide Visibility and Risk Assessment
Consistent Policy Enforcement
Focused on:
Accurate FOSS inventory/catalog
Risk assessment and minimization
Consistent and integrated processes
Minimizing Duplication of Effort
2 Measured
Governance Process Specified
Teams Assess Needs & Manage Selection
Some Awareness of Risks
Focused on:
Best of Breed FOSS
Education
Basic internal support and structures
Basic governance (Policy)
Current Level
1 Exposed
No Defined Governance
Varying Repeated Efforts
Individuals Assess Needs
OSS Selection Unmanaged
Focused on:
Personal Preferences
Small Scale OSS usage
Individual Self Support
Take Advantage of Obvious Opportunities

LF Consulting recommends making investments to improve CLIENT's open source governance program and manage both the legal and operational risks with regards to using and leveraging open source software to achieve company goals. **As a first step, CLIENT should rollout an Open Source Policy that will provide the foundation for the governance program across all business units. The policy should provide guidance to the CLIENT development community on use of OSS and participating with open source communities.** CLIENT should ensure that the OSS policy will sufficiently cover all the aspects needed for an effective management program. The policy should cover all the 8 dimensions of management of open source and not simply address legal compliance. However, care should be taken so that the effort does not result in a policy that is overly complex and therefore be hard use as a basis for the management program.

Furthermore, LF Consulting recommends that CLIENT continue to improve its understanding of industry best practices and develop a plan to improve your governance infrastructure using additional practices and tools. These steps will allow CLIENT to realize greater benefit from open source software and their investment in an open source management program. This will enable CLIENT to better manage the risks and the costs of open source software using industry proven techniques. LF Consulting believes that you will recoup any additional investments in these areas due to risk mitigation and operational efficiency. Implementing these programs will increase the already demonstrable ROI with regards to the use of open source software.

Specific Program Recommendations

For each of the 8 disciplines of management of OSS, LF Consulting recommends that CLIENT consider implementing the following new practices. By incorporating these new practices into your already existing practices, CLIENT will achieve increased value from OSS while reducing both operational and legal risks. Implementing these recommended practices will place CLIENT squarely in the "Participating" level of maturity (or beyond) for all disciplines.

OSS Discovery

- Leverage tools to implement a catalog of pre-approved OSS and direct development teams to first search there.
- Integrate this catalog with approval and validation processes.
- For new OSS, provide formal written guidance on what is acceptable open source to your development teams. Enable them to be able to effectively search for OSS and eliminate unacceptable OSS during the search process.

OSS Review & Selection

- Using a workflow driven system, implement an OSS approval process that goes beyond legal and considers other aspects (Like architecture and security). Automate this process as appropriate.
- Form an *Open Source Review Board* to own this process.

OSS Supply Chain

- Require software vendors to list OSS, provide license text and license compliance requirements.
- Review vendors/partners OSS governance programs, not just the code itself.
- Request vendors/partners with immature OSS governance programs engage in code scanning activities to validate their OSS usage.

OSS Code Management

- Create an internal repository to contain the original, unmodified version of OSS files in use. Make sure you have copies of the source for any OSS downloaded and used in binary format.

- Clearly segregate your OSS & Third Party code from your proprietary code in your source code management systems.
- Integrate your current Open Source historical repositories into your approval processes. Track that components have been inserted into the repository.

OSS Maintenance & Support

- Leverage external tools or subscriptions services to enhance your support/maintenance process by monitoring new releases and vulnerabilities.
- Consider more proactive ways to provide consolidated OSS support. Consider a defined process to identify and manage OSS that should be centrally supported.

OSS Compliance Program

- Create a process by which the compliance obligations for OSS are visible early in the development life cycle so their implementation can be planned.
- Implement code reviews (or code scanning solutions) during your software development phases to verify planned components are the ones in use.
- Implement a formal step in your software development lifecycle during your release that during which compliance to OSS licenses is verified.
- Integrate Legal License reviews (where obligations are determined) with the compliance validation process. Use integrated tools to support the process.

OSS Community Interaction

- Create formal guidelines in which employees may communicate with OSS communities as CLIENT employees (which they currently do today).
- Implement a process by which CLIENT developers can submit bug fixes to OSS communities with minimal, but appropriate management oversight.
- Consider sponsoring OSS or contributing new functionality to existing OSS (not just bug fixes) if this can help drive CLIENT strategy.

OSS Executive Oversight

- Involve executive management in the overall OSS management process. Define approvals (or exception grants) that must be performed by executive management.
- Provide executives reports showing metrics of OSS usage and compliance status.
- Involve Executive Management in the creation of an overall OSS policy. Consider creating an *Open Source Management Board* to own this policy.

Background

About LF Consulting

For over ten years, LF Consulting has helped firms such as IBM, Microsoft, NEC, Intel, Motorola, Nokia, HP, Unisys, and many more develop effective and differentiated open source strategies. Today, LF Consulting is the leading open source business and strategy consulting firm. Our mission is to help clients capitalize on the strategic, technological, and financial benefits of open source software. LF offers a suite of services including; corporate open source strategy development, community building, organizational change management, IP management, compliance, and governance and product and technology development. Our clients include Fortune 500 enterprises, independent software vendors (ISV), start-up firms, venture capital groups, open source governing bodies and government entities.

With over a decade of experience, LF has completed over 500 engagements for more than 200 clients with high profile entities including; Wells Fargo, Bank of America, the US Navy, and the Prefecture of Taiwan. We have built a strong reputation in the venture capital community as well as with dozens of commercial open source startup clients, seven of which were named as Top 10 open source-related business models to follow by industry analyst the 451 Group.

For more information on The Linux Foundation's professional open source management consulting services, and to contact us for an assessment, please visit https://www.linuxfoundation.org/offerings/open-source-management-consulting