TODO

CLOUD NATIVE COMPUTING FOUNDATION

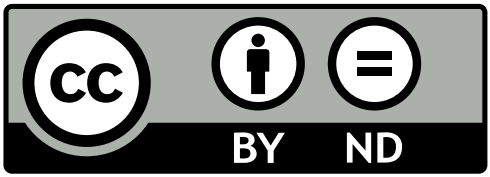
OSPO BOOK

A Guide to Open Source Management and Operations Through Open Source Program Offices (OSPO)

OSPO Book

To reference the work, please cite as follows:

> OSPO Book Contributors, TODO Group. The OSPO Book: A Guide to Open Source Management and Operations Through Open Source Program Offices (OSPO), Version 1.0, May 2025.



CONTENTS

WHAT IS THIS BOOK ABOUT?

Open source is a reality for all organizations that work with software — not just for software companies. Because of this, actively managing open source is becoming increasingly important for many organizations.

One way to manage open source is by setting up an Open Source Program Office (OSPO). Many companies and organizations have adopted this approach, and there is now a lot of shared experience and knowledge about how to do it successfully. In the open source spirit, much of this knowledge is openly available in the community.

This book provides a clear introduction for anyone who wants to understand how OSPOs help organizations manage open source. It's also a helpful resource for people already working in OSPOs who want to strengthen their role in shaping and managing open source strategy and operations. The book offers practical advice on topics such as:

- Building an open source strategy.
- Setting up an OSPO.
- Managing day-to-day operations.
- Collaborating effectively with external open source communities.

What This Book Doesn't Cover

This book doesn't focus on how to develop open source software or explain technical details in depth.

It also doesn't provide step-by-step instructions for using, deploying, or contributing to specific open source software projects.

Who Should Read This Book?

This book is for anyone who wants to understand the role of OSPOs within an organization.

More specifically, it will be useful for:

- Executives, policymakers, and decision-makers who are responsible for setting up, supporting, or funding an OSPO.
- Open Source Program Managers and team leads who coordinate open source activities and build relationships with open source communities.
- Legal and compliance professionals who handle legal matters related to open source, such as licensing and intellectual property.

ABOUT THE CONTRIBUTORS

Each contributor has brought a unique perspective, making the OSPO Book Project v 1.0 possible:

Alin Jerpelea
Ana Jiménez Santamaría
Annania Melaku
Alice Sowerby
Carlos Maltzhan
Chris Aniszczyk
Chris Xie
Christine Abernathy
Cornelius Schumacher
David A. Wheeler
Fernando Eugenio Correa
Gary White
Gergely Csatari
Gil Yehuda
Hiro Fukuchi
Ildiko Vancsa
Jan van den Berg
Jiri Marek
Jonas van den Bogaard
Kate Stewart
Masae Shida
Masayuki Kuwata
Matt Germonprez
Maurice Hendriks
Remy D
Rob Moffat
Ryan Fallon
Seo Yeon Lee
Shane Coughlan
Shilla Saebi
Stephanie Lieggi
Supriya Ashish Chitale
Swastik Baranwal
Takanori Suzuki
Ulises Gascon
Victor Lu

ABOUT THE TECHNICAL REVIEWERS

Alice Sowerby

Alice is a senior operational leader in tech, She's currently self-employed and providing Program Management services to the FreeBSD Foundation. Previous jobs include Program Director for Developer Relations at Equinix, COO at an MLOps startup, and a range of roles in product, engineering, and marketing teams in B2B tech.

What she loves most about work is raising people up through collaborating, coaching, mentoring, and servant leadership. Her strategic and problem-solving skills mean she is valued as a key member of many groups. She is an elected member of the Steering

Committee in the TODO group, and is the lead editor for the OSPO Book project. She also co-produces and host the CHAOSS project's podcast, CHAOSScast.

Alice is based in the UK, in a small village near Bath. She enjoys travel, languages, gardening and science.

Fernando Eugenio Correa

Fernando is a professional with over 25 years of experience in software development, having held roles such as team coordinator, technical lead, software engineer, and systems analyst. He has worked on ERP systems, financial transactions involving debit and credit between financial institutions and ATMs/POS devices, ISO8583 protocol, serial communication, TCP/IP, embedded software, and games.

Since 2022, he has been part of MercadoLibre's OSPO, with great involvement in compliance, training open source business strategy and community engagement, as well as remaining deeply committed to promoting and supporting innersource. Committed to fostering open source and innersource culture and communities in Latin America.

TODO OSPO Ambassador and Member of the InnerSource Commons Foundation.

Jan van den Berg

Jan has been scripting since childhood, which naturally evolved into a passion for software development. He is a quick learner, particularly when it comes to IT-related matters.

He began his professional career in 2001 as a webmaster for two years, followed by four years as a Network Services Administrator. Since 2007, he has worked as a Java developer on various projects across multiple companies. In 2020 he became a Site Reliability Engineer and moved on to a Staff Engineer role in 2024.

Committed to staying up-to-date with the latest technologies, Jan has explored a range of programming languages including Perl, PHP, Python, Node.js, Scala, Clojure, Kotlin, C, Go, Rust and Zig. He also completed the Machine Learning course on Coursera with top marks.

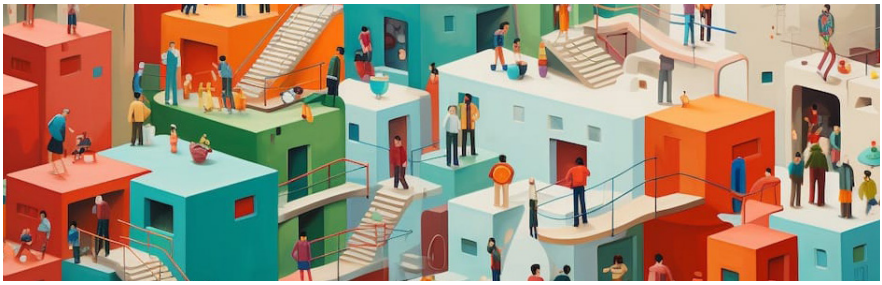
CHAPTER 1: INTRODUCTION TO OPEN SOURCE PROGRAM OFFICES

Introduction

In today's digital ecosystem, open source resources have transformed from a niche technical approach to a foundational element of modern organizations' technological infrastructure. Companies across sectors increasingly rely on open source components, frameworks, and tools to drive innovation, reduce development costs, and accelerate time-to-market for their products and services. However, this growing dependence introduces complex challenges related to security, compliance, licensing, and strategic alignment that require deliberate management rather than ad-hoc approaches.

The Open Source Program Office (OSPO) has emerged as a critical organizational function designed to strategically navigate these challenges. An OSPO acts as the centralized hub for an organization's open source activities, coordinating usage policies, contribution strategies, compliance procedures, and community engagement initiatives. By establishing formal governance structures, OSPOs enable organizations to systematically manage risk while maximizing the business value derived from open source technologies and communities.

Beyond risk management, successful OSPOs fundamentally transform how organizations interact with the broader open source ecosystem. They foster internal engineering excellence through knowledge sharing, promote external recognition through strategic contributions to key projects, and create pathways for innovation by maintaining healthy relationships with open source communities. Organizations that implement well-structured OSPOs typically experience enhanced developer productivity, improved software quality, reduced legal exposure, and strengthened competitive positioning in talent markets where open source expertise and values are important.



About OSPOs

Defining an OSPO

An OSPO is designed to do the following:

1. Be the center of competency for an organization's open source operations and structure, and
2. Place a strategy and set of policies on top of an organization's open source efforts. This can include setting code use, distribution, selection, auditing, and other policies; training developers; ensuring legal compliance; and promoting and building community engagement to benefit the organization strategically.

OSPOs can vary across organizations. For example, OSPOs may be situated in the R&D department, in the office of the CTO, in the Engineering department, or be "virtual" meaning that it's made up of people from across the business. An OSPO can be large and multi-layered for example, a corporate OSPO with division-level OSPOs or it can be much smaller. It can even be an informal, self-organized group.

> NOTE: For a more in-depth explanation of OSPOs see the TODO Group's official definition of an OSPO, linked to in the Resources and Footnotes section of this chapter.

How an OSPO Works Inside an Organization

OSPOs have a very strong role in creating cross-functional collaboration in an organization. This involves integrating open source practices into interactions with various internal and external open source stakeholders that have a direct or indirect impact on the OSPO. Demonstrating the value of open source when integrating it as part of the overall digital strategy is important to achieving shared organizational objectives.

An OSPO considers cross-functional collaboration from four different perspectives:

- Looking downward: The head of an OSPO must manage the team's tasks effectively. Depending on the OSPO's objectives, the team's responsibilities may vary.
- Looking upward: If proposing the creation of an OSPO, managing expectations and aligning with executives' technology needs is necessary.
- Looking sideways: Collaboration with other teams is critical. For instance, in business-oriented OSPOs, collaborating with the developer tools and security teams is essential.
- Looking outside: Representing the organization to external communities and foundations is crucial. The integration strategy must align with the organization's objectives and vision.

As an example, the following diagram illustrates the various players in a business-oriented OSPO and the different methods of cross-functional collaboration.

History

In the past, collaborative OSS development was primarily adopted by small groups of developers and enthusiasts, and there was little need for dedicated organizational units to manage open source activities. However, as this method has become more prevalent and critical to the operation of many organizations, the need for dedicated OSPOs has become more apparent.

The OSPO concept initially started within the corporate world about two decades ago, but adoption accelerated significantly in the last decade. Most prominent technology infrastructure firms (for example Amazon, VMware, Cisco) and consumer technology companies (for example Apple, Google, Meta (formerly Facebook)) have created OSPOs or formal open source programs. All are encouraging their employees to contribute to open source projects that are strategic to their business and security.

The term “OSPO” has become more mainstream and diverse in the last few years, as more organizations from different sectors and regions have created dedicated open source roles in their organization to manage open source operations and strategy. Recently, OSPOs have been formed in different regions (APAC, EMEA, AMER) and different types of organization, such as governments, enterprises, NGOs, and universities.

> NOTE: In this book we refer to the part of the organization managing open source as an OSPO, but depending on your organization you might use a different name. OSPOs vary depending on sector, region, organizational size, and many other factors. The name may exclude the term 'Program' to become 'Open Source Office' or you may use a completely different name such as 'Open Source Center of Competence', 'Open Source Steering Committee" or 'Open Source Software Team'.

Applying This to Your Organization

Does Your Organization Need an OSPO?

Now that we understand something about the purpose and nature of OSPOs, it's a good moment to consider how this might apply to your organization. If your organization doesn't have an OSPO yet, your first step is to determine if an OSPO is the right solution for your organization's needs based on its existing open source engagement level, culture and understanding.

While this is a book about OSPOs, it's important to note that establishing an OSPO might not be the starting point for open source operations. Before establishing an OSPO, companies and organizations need to assess their current goals, and their relationship with OSS projects.

> NOTE: Chapter 3 contains more information to help you decide what your OSPO should look like and how to get it started.

Understand the Role of Open Source in your Organization

The first step in assessing whether your organization needs an OSPO is to find out the current level of open source resources used, contributed, or produced in the organization. This information is important when you are thinking about how an OSPO can help your organization manage the risks and opportunities that come with open source. The OSPO can help to ensure that open source activities in your organization are effectively managed and aligned with strategic goals and objectives.

Assessing open source adoption is critical because it sets the foundation for successful open source operations. Without proper understanding and adoption of open source, an OSPO may not be effective in achieving the
desired outcomes.

Consider the following areas of open source engagement in your organization:

- **Open Source Software Usage:** Evaluate the level of OSS usage within your organization. Are there any specific open source projects that are widely used? Are there any projects that are critical to the organization's operations?

- **Knowledge and Understanding of Open Source:** Evaluate the level of knowledge and understanding of open source within your organization. Are the different actors that will be or are currently involved in open source familiar with open source licensing models and requirements? Do they understand the benefits and risks of using OSS?
- **Culture:** Evaluate the culture within your organization to determine if it's conducive to open source operations. Is there a culture of collaboration and sharing? Are the different actors that will be or are currently involved in open source willing to contribute to open source projects?
- **Tools and Processes:** Evaluate the tools and processes in place to support open source operations. Are there any existing tools or processes that can be leveraged for open source operations? Are there any gaps in tools or processes that need to be addressed?
- **Addressing Gaps:** Determine if there are any gaps in open source adoption or readiness and develop a plan to address them. This may include training those actors that will be or are currently involved in open source on OSS usage and licensing, developing new tools and processes to support open source operations, or establishing an OSPO to coordinate open source activities.

Overall, gather input from stakeholders on these areas by asking the following questions:

- How would you define 'open source'?
- What does 'open source' mean for you and your organization?
- How much OSS is already being used in the organization?
- How would you define the 'open source culture' within your organization?
- What are the organization's goals and objectives for using open source?
- How is OSS currently being used within the organization?
- How is OSS currently being created within the organization?
- If any, what are the current policies and procedures for managing OSS within the organization?
- What are the key legal and compliance considerations for using OSS within the organization?
- What are the motivations for implementing an OSPO within the organization?
- What are the challenges of implementing an OSPO within the organization?
- What resources and support will be needed to successfully implement an OSPO within the organization?

Conclusion

An OSPO can help many organizations achieve better outcomes with open source. Understanding your organization's needs and its current use of open source are a great place to start when considering creating an OSPO.

Possible Problems and How to Overcome Them

PROBLEM	RECOMMENDATION
The OSPO is established without proper alignment with organizational goals. This can lead to difficulty in making progress.	When setting up the OSPO, ensure that you understand the organization's needs. Then establish a clear mission for the OSPO, set measurable objectives, and foster cross-departmental collaboration.
The OSPO is seen as a separate silo within the organization.	Take the time to identify the OSPO's internal and external stakeholders and know what you intend to deliver for them and your organization. This will require integrating open source practices into various departments, and demonstrating the value that open source brings in achieving shared organizational objectives.
The OSPO is seen as a legal or compliance function only.	Take care to position the OSPO beyond merely legal and compliance roles by emphasizing its strategic importance in providing support to achieve organizational goals, meet both external and internal security regulations, and foster innovation.
The OSPO is seen as a one-size-fits-all solution.	Carefully assess the specific needs and objectives of your organization to determine if an OSPO is the right fit, tailoring its structure and functions to effectively align with your unique organizational goals and strategies. Share the mission of your OSPO, and demonstrate how your work delivers on that mission.

Resources

- OSPO definition: **https://github.com/todogroup/ospodefinition.org**
- Source of the diagram: **https://lists.todogroup.org/g/WG-ospo-book-project/message/5**
- ML discussion: **https://lists.todogroup.org/g/WG-ospo-book-project/message/5**
- OSPO 101 Module 1 - **Open Source Introduction: https://github.com/todogroup/ospo-career-path/tree/main/OSPO-101/module1**
- OSPO 101 Module 2 - **Open Source Business Models: https://github.com/todogroup/ospo-career-path/tree/main/OSPO-101/module2**
- OSPO 101 Module 3 - **Open Source management & your organization: https://github.com/todogroup/ospo-career-path/tree/main/OSPO-101/module3**
- OSPO easy FAQ - TODO Group and Open Chain Japan, Linux Foundation: **https://todogroup.org/resources/guides open-source-program-office-ospo-easy-faq/**
- How to create an OSPO - TODO Group, Linux Foundation: **https://todogroup.org/resources/guides/how-to-create-an-open-source-program-office/**
- OSPO Definition - TODO Group, Linux Foundation: **https://ospoglossary.todogroup.org/ospo-definition/**
- The OSPO: A New Tool for Digital Government - Open Forum Europe: **https://openforumeurope.org/wp-content/uploads/2022/06/The-OSPO-A-New-Tool-for-Digital-Government-2.pdf**
- **OSPO Adoption Landscape - TODO Group, Linux Foundation: https://landscape.todogroup.org/**
- Business Success with Open Source - VM (Vicky) Brasseur: **https://pragprog.com/titles/vbfoss/business-success-with-open-source/**

CHAPTER 2: THE VALUE OF OPEN SOURCE PROGRAM OFFICES

Introduction

Your organization probably already has a relationship with open source, even if it's not aware of it. Almost all software produced today includes open source components, or is developed or hosted using open source tools. Even organizations that don't make software usually use software that contains open source components.

For many organizations, it's worth considering how actively managing their relationship with open source can bring benefits and reduce risks. As mentioned in the previous chapter, this involves understanding the current use of open source and then assessing how this could be managed better to support organizational goals.

This chapter will help you to understand the possible areas where managing open source through an OSPO can bring value to your organization. This will be different for every organization, so knowing your organization's strategy and goals is important.

The work of an OSPO is to understand where open source can bring value to its organization, and to actively manage or oversee all related activities.

Every organization will have its own reasons for wanting to start an OSPO, some common reasons given in the business value of the *OSPO report 1*[1] are as follows:

- Building standardized processes around open source
- Learning how to approach the open source community
- Embracing the sustainability of open source projects
- Managing compliance
- Expanding access to open knowledge
- Improving development velocity
- Mitigating security risks

1 Business value of the OSPO report: **https://www.linuxfoundation.org/research/business-value-of-ospo**

How Could Your OSPO Add Value?

If You Make Software

This is a common and relatively comprehensive use case for an OSPO. Other organizations may only need to consider a subset of these issues.

Sometimes, organizational stakeholders assume that their product isn't using any open source components because their end product isn't open source. However, when you look at the entire software supply chain you can see that nearly all software contains open source dependencies or artifacts. If the contributors working on those open source projects decided to leave, the project could become obsolete or a target for security vulnerabilities. This affects any software the organization uses or sells, and could directly impact its reputation, performance, or revenue.

An OSPO can help by understanding and actively managing use of open source components in your software.

How the OSPO Helps

- **Managing Vulnerabilities**: Open source projects can be a source of security vulnerabilities in a product that depends upon them. It can be hard to keep track of how open source projects are being used by your organization and to perform risk assessments on the identified projects. When you identify key projects within the organization, you can prioritize securing them by tracking common vulnerabilities and exposures. Often, the Enterprise Architecture team are the ones tracking the open source components of applications and technologies, and OSPOs are there to give subject matter expertise.
- **Understanding Risks in the Supply Chain:** The open source landscape is large and decentralized, and it can be hard to identify who the contributors to individual projects are and to perform risk assessments on the identified projects. These factors can make it challenging for organizations to accurately assess risks and to comprehend the security and quality standards of the software, hardware, data, etc.
- **Building Healthy Relationships with Key Open Source Projects:** Commercial organizations that are using open source are often keen to contribute back to the projects they use. However, the pressure to ship features in their own products means that open source contributions may take a back seat when things get busy. Even when it's known that contributing features and bugfixes to upstream is less effort in the long term than to maintain a fork of the project, organisations often optimize for short term benefits and don't spend the extra effort to upstream the changes.

- **Supporting and Influencing Key Open Source Projects:** Your organization could be in a good position to provide resources to open source projects. That could be through coding, expertise, or money donations as incentives for fixing common vulnerabilities. It could also be productive to collaborate with industry working groups to address security concerns holistically. Making a plan that aligns with your organizational strategy and provides value to the open source projects is a good way to be a helpful community member.
- **Bridging the Gap Between Regulated Processes and Open Source Processes:** Open source is a dynamic ecosystem whose contributions should occur as smoothly and naturally as possible. The long procurement processes faced in highly regulated environments, such as finance companies and governments, create a barrier to open source contribution and engagement.
- **Improving Open Source Literacy to Ensure a High-Benefit, Low-Risk Approach:** The concept of open source may not be taken seriously in other areas of the organization involved in decision-making processes, management, or policy making. This will require constant education and demonstration of the risks and value of open source in the organization.

To get the most benefit from open source, and to reduce the risks, organizations must invest in properly managing open source operations on both cultural and practical levels. This is often accomplished through the OSPO, as it fosters committed, cross-functional collaboration within the organization to address open source issues encountered by various teams or departments. The OSPO operates as a center of excellence.

If You Deliver Public Services

How the OSPO Helps

We see that more public sector organizations are realising the value of an Open Source Program Office to achieve their digital policy goals to better serve their citizens, and to transform their organizations toward achieving these goals.

Public sector organizations face unique challenges when it comes to managing their open source operations, including the need to comply with strict laws and regulations, and the requirement to provide transparent and accountable operations. An OSPO can help governments and public sector organizations to overcome these challenges.

Improving Compliance: An OSPO helps to ensure that their open source operations are compliant with relevant laws and regulations, including data privacy laws, procurement regulations, and transparency requirements. This helps organizations to avoid costly legal and regulatory challenges and to maintain their reputation as responsible public sector organizations.

Increasing Collaboration: An OSPO helps to foster collaboration between different departments and with external stakeholders, including other public sector organizations, open source communities, and civil society organizations. This increased collaboration helps organizations to access a wider pool of talent and resources, and to develop better open source solutions.

Improving Resource Allocation: An OSPO helps to allocate resources more effectively, ensuring that open source operations are well-supported and that key initiatives are given the resources they need to succeed. This helps organizations to maximize the benefits of open source technology and drive innovation and growth.

Improving Service Delivery: An OSPO helps to improve the delivery of public services, by enabling them to adopt innovative and cost-effective technologies, and to collaborate with external stakeholders to develop better solutions. This helps organizations to provide better services to citizens and to meet the changing needs of their communities.

The European Commission's Open Source Program Office (OSPO) has launched a new portal that serves as a wiki or knowledge archive, providing up-to-date information on advancements in OSPO-related topics for public administrators. This portal offers a variety of resources, including useful studies, presentations, use cases, guides, and more, to readers interested in learning more about OSPO-related topics. See the Resources section at the end of the chapter for a URL.

As a Cultural Influence

In a world governed by software, Open Source Program Offices (OSPOs) serve as powerful cultural catalysts within organizations. Beyond simply managing technical integration of open source solutions, OSPOs fundamentally transform organizational culture by fostering open collaboration, transparency, and innovation.

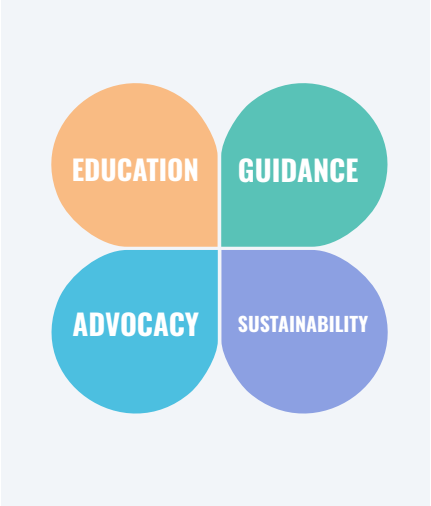
As organizations increasingly rely on open source for mission-critical problems — whether social, economic, or technological — the OSPO's cultural influence becomes essential in reshaping mindsets and workflows. This cultural shift enables organizations to move beyond viewing open source as merely a resource to extract value from, toward becoming active, contributing members of the broader open source ecosystem. By embedding open source values and practices throughout an organization, OSPOs cultivate internal champions, establish collaborative norms, and nurture a culture where knowledge sharing thrives.

This cultural transformation not only supports risk management and innovation but ensures the sustainability of the open source communities they depend on. Without an OSPO's ongoing cultural influence, organizations risk losing open source expertise, increasing security and legal vulnerabilities, reducing community engagement, and damaging their reputation.

Open Source is a silent critical need, and an OSPO's cultural impact is vital to evolve organizational culture and knowledge, helping to build more secure and sustainable OSS.

How the OSPO Helps

Acts as a Counselor: Sometimes a strategic approach just means stepping back and taking the time to think through some of the hard questions about what type of engagement model is right for any particular project or how involved the organization should be in each project. There is also the question of when it makes sense to contribute to an existing project versus creating a new project. An OSPO that is having these strategy-level conversations will be able to provide guidelines to workers at the different teams so that workers don't have to consider the business implications of different open source engagement models every time they try to solve a problem.



Acts as a Facilitator: The OSPO also plays a sort of translation role between the organization's teams and decision makers' interests regarding open source and the needs from the open source community. They also help organizations navigate the cultural, process, and tool changes required to engage with the open source community effectively and in a healthy way.

Acts as an Advocate: OSPOs can promote the use of open source and its best practices across different organizational units. This can help organizations realize the benefits of open source as well as engage people to contribute to open source projects or start new ones.

Acts as an Environmentalist: OSPOs can help organizations support and sustain open source projects in the long term by addressing issues such as security, maintenance, and project health. This can help ensure that open source projects remain healthy in the long term and continue to benefit the wider community.

Acts as a Gatekeeper: OSPOs can help enforce open source policies and strengthen open source governance. This can help organizations to ensure compliance and mitigate open source security risks.

As an Intermediate Step to a Decentralized Open Source Management Model

OSPOs help manage open source as an ongoing activity and work to integrate it well into all an organization's units. Some organizations are going a step further to take ownership of the full management of open source within their regular structures and functions. There is an open question related to whether the OSPO would become an intermediate step to achieve this.

The answer depends on how you view the OSPO. Beyond the multiple different structures an OSPO can have, it's fundamentally about its people. An OSPO is a group of open source subject matter experts providing support, knowledge, and management related to all open source activities. These people must be not only retained but also reinforced and effectively financed for the future, as more open source integration is inevitable.

In an ideal scenario, open source knowledge, technical expertise, and culture should be integrated as any other employee skill. However, the reality is that this is a long way from happening. Currently, it's challenging to find open source experts who can effectively bridge the gap between open source communities and specific work units (for example: security, legal and business), let alone enough people to place in every part of the business.

However, what might change in the coming years is the centralized view of the OSPO. This traditional perception may diminish, leading to more decentralized structures across teams and business units.

[Source: OSPOs, key lever for open source sustainability][1]

1 Business value of the OSPO report: **https://www.linuxfoundation.org/research/business-value-of-ospo**

Applying This to Your Organization

Assess the Value of Open Source Use

Organizations may underestimate how much they already depend on the usage of open source. Several studies analyze the usage of OSS in the industry. For example, the Synopsys Open Source Security and Risk Analysis Report 2024[3] finds that the average software project consists of 77% OSS. Additionally, *a Harvard Business School study*[4] estimates that the supply-side value of widely-used OSS is $4.15 billion, while the demand-side value is much larger at $8.8 trillion. Moreover, a study by *OpenForum Europe*[5] estimates that OSS contributes between €65 to €95 billion to the European Union's GDP and promises significant growth opportunities for the region's digital economy.

Assess this value for your own organization by taking steps such as:

- Collecting information about what OSS is used by your development and operations teams.
- Getting a clear view of what open source components are in the commercial software you buy or services you use. Ask vendors for what OSS they use, for example by requesting Software Bill of Materials (SBOMs).
- Assessing the cost savings of current open source use by evaluating what it would cost if you had to replace it with commercial alternatives.
- Evaluating how using existing open source components can increase the speed of innovation or engineering agility.

Consider what Value Your OSPO Might Bring in the Future

The value of an OSPO to your organization may increase over time as strategy and goals of your organization change. Your OSPO should regularly review its value to the organization, and plan to increase its maturity level if needed. More information about OSPO maturity is available in Chapter 3 where the topic of Maturity Models is introduced.

---

3 Synopsys Open Source Security and Risk Analysis Report 2024: **https://www.synopsys.com/content/dam/synopsys/sig-assets/reports/rep-ossra-2024.pdf**

4 Harvard Business School study: **https://www.hbs.edu/ris/Publication%20Files/24-038_51f8444f-502c-4139-8bf2-56eb4b65c58a.pdf**

5 Study by OpenForum Europe: **https://openforumeurope.org/publications/study-about-the-impact-of-open-source-software-and-hardware-on-technological-independence-competitiveness-and-innovation-in-the-eu-economy/**

Communicate With Stakeholders

When communicating the value of your OSPO to your organization, the best route forward is to present the top 2-3 areas of value that are most clearly aligned to organizational strategy. There may be many other areas where the OSPO adds value but research shows that a long list of benefits can weaken the business case rather than strengthen it (you can search for the "Weak Argument Effect" online for more information). Work on a clear, compelling short value proposition that will cut through, and use it as an anchor for presenting the OSPO in all situations.

Don't rely on general "good practice" arguments. Though these may be based in truth, they're not usually very compelling and don't help to build strong buy-in across the organization.

Don't rely on the value of your OSPO meeting speculative future needs. It's great to be prepared, but unless there is a clear initiative that's about to start which your OPSO can help with, it's better to focus on the value you can deliver here and now.

Examples of the OSPO's value

To illustrate how your OSPO may deliver value to your organization, some example stories can be a great way to build buy-in. Here are two examples where an OSPO could be vitally important:

Managing a Vulnerability in the Software Supply Chain

For example: a social engineering attack targeted the xz/liblzma[6], an essential open source library. The attack was meticulously planned, gaining trust within the community before executing a malicious attack. This incident was discovered inadvertently by an unrelated project, underscoring the sophistication and stealthiness of such vulnerabilities. The challenge for OSPOs lies in identifying and mitigating these vulnerabilities, which are not always apparent until after they occur. Despite existing procedures and policies, OSPOs recognize the need for mechanisms to proactively measure and respond to such threats.

How the OSPO Helps

- **SBOMs Compliance Ready**: Ensure that all software components are documented through automatically generated Software Bill of Materials (SBOMs). This documentation helps quickly to identify potentially compromised components once a vulnerability is disclosed.

6 Social engineering attack targeted the xz/liblzma: **https://research.swtch.com/xz-timeline**

- **Automated Security Checks: I**mplement automated security checks, such as the OpenSSF Scorecard[7], to continuously evaluate the security posture of projects. This proactive measure can highlight vulnerabilities or anomalies that merit further investigation.
- **Having a Computer Emergency Response Team (CERT)** within the organization and having the OSPO collaborate closely with them. This specialized team should be equipped with the tools and authority to respond swiftly to security incidents. Pre-existing relationships within the team facilitate rapid internal communication about the severity of incidents.
- **Scorecard Management:** Keep security and vulnerability scorecards up to date. These scorecards should reflect the latest security checks and assessments, helping in quick decision-making during a crisis.
- **Automated Feedback Loops:** Develop well-automated feedback loops for bug reporting and fixing. Knowing who is responsible for addressing a particular bug and ensuring that this process is as automated as possible can significantly reduce response times.

Managing a Licence Change in the Software Supply Chain

OSPOs face the challenge of navigating license changes and assessing software trustworthiness. When projects like Redis change their terms[8] it can have significant implications for use, distribution, and contribution. OSPOs need to communicate these changes clearly and understand the roles and responsibilities dictated by new license terms. Furthermore, OSPOs are tasked with evaluating the trustworthiness of software, which can vary based on whether a project is maintained by a single vendor or hosted under a foundation. For instance, The AlmaLinux OS Foundation[9] presents a case where donating a project to a foundation mitigated risks associated with single-vendor governance, thereby enhancing trust in the project.

How the OSPO Helps

- **Educational Initiatives on License Implications:** Develop educational materials and sessions for developers and users within the organization to understand the nuances

7 OpenSSF Scorecard: **https://scorecard.dev/**

8 Redis changes their terms: **https://www.theregister.com/2024/03/22/redis_changes_license/**

9 AlmaLinux OS Foundation: **https://thenewstack.io/jack-aboutboul-how-almalinux-came-to-be-and-why-it-was-needed/**

of different licenses. This understanding will help them make informed decisions when using or contributing to open source projects.

- **Explicit License Terms:** Work with legal teams to ensure that license terms are as explicit and unambiguous as possible. Clear terms help in avoiding misunderstandings and potential legal conflicts.
- **Software Trust Rating System:** Implement a system to evaluate and rate the trustworthiness of software, considering factors like governance structure, maintenance practices, and community engagement. Projects hosted under reputable foundations could be rated higher for trustworthiness due to the oversight and governance provided.
- **Encourage Foundation Hosted Projects:** Advocate for donating projects to foundations to mitigate risks associated with single-vendor control. Highlight successful cases like AlmaLinux to illustrate the benefits of this approach, such as increased trust and community support.
- **Stakeholder Engagement in License Decisions:** Engage a broad range of stakeholders, including developers, legal advisors, and end users, in discussions about license changes or the adoption of new projects. Their insights can help in making balanced decisions that align with the organization's values and risk tolerance

Possible Problems and How to Overcome Them

In this section, you will find a series of real-world scenarios that are encountered in open source management across organizations. For each scenario, you can find recommendations from real-world experiences from open source professionals.

PROBLEM	RECOMMENDATION
There is a lack of understanding about open source practices across the organization.	It can be hard to demonstrate the value of the OSPO if there is a poor understanding of open source in the organization. Focusing on speaking about your key areas of value and using the power of stories will help you to build understanding quickly in the organization. Sharing real-world stories about how your organization is using open source, and sharing cautionary tales about times an OSPO saved an organization from a risk can help to educate people through easily repeated narratives. As time goes by, you can start to promote better organizational-wide understanding of open source practices by offering educational workshops, creating accessible resources, and establishing open source champions in different departments to foster a culture of open source literacy.

PROBLEM	RECOMMENDATION
The OSPO's value is seen as a sales profit or marketing tool.	Because the OSPO has a role in supporting relationships with open source communities and partners, it can be natural for sales and marketing to see some value to them in this engagement. As an OSPO you can only fulfill your responsibilities by building trust with third parties over time. Set boundaries with sales and marketing and say "no" to things that might reduce your reputation in the ecosystem. Work on building internal understanding of the OSPO as an integral part of the organization's digital, software, or IT strategy, and highlight work that fosters open source best practices, contributes to technological innovation, and supports the overall organization's goals.
The OSPO's value is seen as secondary or discretionary, and not as critical for the organization's core functions.	The cause of this problem is either that the OSPO isn't aligned with the organization's needs, or that the OSPO isn't communicating its value well. Review the OSPO's value, and plan your communications to highlight how the OSPO enhances key business processes, drives innovation, and directly supports strategic objectives, thereby integrating it as an essential component of the organization's operational framework.
The OSPO struggles with gaining executive support and buy-in.	Executives require a particular type of communication. They need to have a clear picture of the role and value that each part of the orgnization brings. If the message is too detailed or vague, or if the subject is too specialist they can struggle to "get it". As the OSPO, you need to communicate the strategic value of open source and of the work the OSPO does to manage it. Showcasing visible benefits through case studies, success stories, or numerical reports can help to cut through with a clear and simple presentation that demonstrates OSPO initiatives are delivering with key organizational priorities

Resources

- Log4Shell real vulnerability example: **https://en.wikipedia.org/wiki/Log4Shell**
- Open source and the software supply chain - John Mark Walker: **https://opensource.com/article/16/12/open-source-software-supply-chain**
- Strategy: End Game for FINOS Maturity Model - Victor Lu: **https://docs.google.com/presentation/d/1jJtR6-fvU-dCrGq_gTm4P1Awv90oCu4RClj1919970A/edit#slide=id.g1ed9ae7029f_0_29**
- Securing the Software Supply Chain: The Role of OSPOs - Jessica Marz: **https://www.intel.com/content/www/us/en/developer/articles/community/securing-software-supply-chain-the-role-of-ospo.html**
- Simple Frequently Asked Questions OSPO Guide - OSPO SWG Japan: **https://qiita.com/owada-k/items/017d1b98d0e437766bd0**
- The Business Value of the OSPO Report - Linux Foundation: **https://www.linuxfoundation.org/research/business-value-of-ospo**
- EC Open Source Programme Office - European Commission Joinup: **https://joinup.ec.europa.eu/collection/ec-ospo**
- Public Services Should Sustain Critical Open Source Software - FOSSEPS: **https://joinup.ec.europa.eu/collection/ec-ospo**
- How Governments Want to Use OSPOs to Transform Themselves - Sivan Pätsch: **https://joinup.ec.europa.eu/collection/open-source-observatory-osor/news/growing-case-ospos-government**
- Open Source Security and Risk Analysis Report 2022 - Synopsys: **https://www.synopsys.com/software-integrity/resources/analyst-reports/open-source-security-risk-analysis.html**
- Open Technology - Scheerder, Jeroen & Koymans: **https://www.researchgate.net/publication/254920512_Open_Technology#pf7**
- The Pros and Cons of Open Source Software - Khalil Khalaf: **https://medium.com/@kylekhalaf/the-pros-and-cons-of-open-source-software-d498304f2a95**

CHAPTER 3: CREATING YOUR OSPO

Introduction

OSPOs can be really diverse, so taking the time to design an OSPO that will deliver on your organization's goals is important.

This chapter will first help you to idenify your strategy so you can have a basis for planning the work your organization should do, and how the OSPO should be structured.

It will then look at designing and building a stable and strong OSPO that's capable of covering the open source-related tasks and responsibilities needed by your organization.

Lastly, this chapter will introduce maturity model as a way of understanding what's appropriate for your OSPO now and in the future as needs change.

Starting With Strategy

How To Develop Strategy

> For individuals in Open Source Program Offices, effectively communicating the open source strategy to C-level executives demands a keen understanding of the industry landscape and alignment with the key considerations of CEOs and CFOs. This alignment necessitates a clear comprehension of the overarching corporate strategy and identifying technologies within the open source realm that can propel the organization toward its strategic objectives.
>
> Victor Lu and Rob Moffat Presentation - Strategy - End Game for FINOS Maturity Model[10]

An OSPO achieves this by creating and maintaining a framework covering the following aspects: strategy, governance, compliance, and community engagement. The OSPO's strategy focuses on aligning the organization's open source use, contributions and compliance activities to its overall organization objectives across its projects, products, services, and internal infrastructure.

A strategy creates a high-level consensus on concrete topics and their impact on your organization and the people within it.

10 Strategy - **End Game for FINOS Maturity Model: https://osr.finos.org/docs/presentations/strategy**

Things to consider when creating your strategy:

1. **Create a strategy document:** A good practice is to document this strategy in an open source strategy document[11]. This guide takes you through the process step-by-step.
2. **Understand your Organization's Goals:** As mentioned in the previous chapter, you will need to understand your organization's goals, and its current engagement with open source.
3. **Consider the Context:** When developing your OSPO's strategy and design, you have a few different ways to approach its structure and position in the org chart before you think about personnel, technology, and budget. There is an excellent guide produced by the TODO group, called A deep dive into OSPOs[12] which explains all essential information on OSPO structures and operations.
4. **Review an example OSPO's structure:** To get an overview of the potential activities of an OSPO you can review the OSPO Mind Map[13]. This outlines the main responsibilities, roles, behaviors, and team sizes within the ecosystem of an OSPO.

Designing Your OSPO

Identifying What Your OSPO Should Manage

To do a good job, an OSPO needs to understand how the organization works. Knowing the company's goals helps the OSPO make informed choices about using open source. For example, in a business setting, an OSPO might look at these areas to see how open source fits in:

11 Creating an open source strategy document: **https://todogroup.org/resources/guides/setting-an-open-source-strategy/**

12 A deep dive into OSPOs: **https://www.linuxfoundation.org/research/a-deep-dive-into-open-source-program-offices**

13 OSPO Mind Map: **https://todogroup.org/resources/mindmap/**

Since every organization is unique in its values, business drivers, and culture, it's challenging to provide specific content. However, addressing the following questions can help structure the document effectively:

- Which open source technology is and which will be important for your organization's goals and product roadmap?
- Which open source projects directly and indirectly develop or influence these technologies and your organization's goals?
- Which specific practices can best foster a sustainable open source ecosystem?
- Which of the organization's processes have areas for improvement?
- How can open source support those improvements?
- How can you make workers champions for open source?
- How can the message be effectively transmitted to management for their understanding?

Taking the time to understand where the OSPO can add value will then help you to recognize who your stakeholders are.

Identifying Your OSPO's Stakeholders

There are some common parts of the business where an OSPO may find its stakeholders. Stakeholders are all the people who will be affected by the work you will do. The OSPO flower diagram helps to visualize the different stakeholder groups. Each petal represents a certain group of stakeholders with specific activities associated with this group. The OSPO Flower Diagram can also be used to help you map the specific communication channels, documentation and other material used with each group of stakeholders.

Depending on the complexity of your organization and the resources available to your OSPO, these petals can become more granular and include additional petals with different names.

- **Individual Contributors:** This petal represents the people who the OSPO will work within the organization, focusing on the intrinsic and extrinsic motivators of contributing to open source from an individual point of view. It requires a cultural change effort and may involve activities such as establishing mentoring programs.
- **Management:** In this petal, the OSPO focuses on strategy and finding alignment between open source and the overall business/organization strategy. Managers face unique challenges, and using the strengths of open source helps them overcome these challenges effectively.
- **Legal:** This petal represents the legal aspects of open source. It deals with understanding and managing legal requirements and obligations related to open source initiatives within the organization. This ensures compliance and reduces legal risks.
- **Business:** This petal focuses on how the OSPO ensures all the pieces of the organization structure fit together. It involves sharing best practices across different business/team units and fostering collaboration and knowledge transfer.
- **Open Source Ecosystem**: This petal represents the broader open source community and project ecosystem outside the organization. The OSPO engages with this ecosystem, which includes other organizations, projects, and individuals, to exchange ideas, collaborate, and contribute to the larger open source community.
- **OSPO:** This represents the inner workings of the OSPO itself. The people within the OSPO collaborate and coordinate all the open source initiatives within the organization. They oversee the activities, ensure smooth operations, and provide guidance and support to other stakeholders involved in open source.

Collaborating With External Regulators

External regulators aren't included in the flower diagram, as this is a special case.

Organizations are subject to various external regulators that influence and shape their policies and processes. These regulators ensure compliance with legal requirements, ethical standards, and industry-specific guidelines. Some external regulators include:

- Government Agencies: Government bodies establish and enforce laws and regulations that impact organizations.
- Industry Regulators: Many industries have their own regulatory bodies or professional associations that set guidelines and standards for organizations to follow.
- Consumer Protection Agencies: Consumer protection agencies ensure that organizations provide fair and safe products or services to consumers.

For open source to be successful and sustainable within an organization, it's crucial to collaborate not only with the open source community but also with external regulators. This collaboration ensures a clear understanding of open source principles when creating policies that affect the ecosystem. The primary objective is to work together and make informed decisions by fully grasping the implications of open source and its community. Thus, it's recommended that the OSPO consider ways to develop a plan for approaching and communicating with regulators, clearly defining the roles they will play in the policymaking process.

Using Maturity Models for OSPOs

An Introduction to Maturity Models

An organization's engagement with open source typically sits along a scale from tactical to strategic. Maturity models help you to understand where on this scale different parts of the organization sit and to have conversations about whether it's in the right place.

There are many different open source maturity models. Some are general, some are specialized. There are maturity models for governments, NGOs, Enterprises and more, with versions and sub-versions to fit any organization.

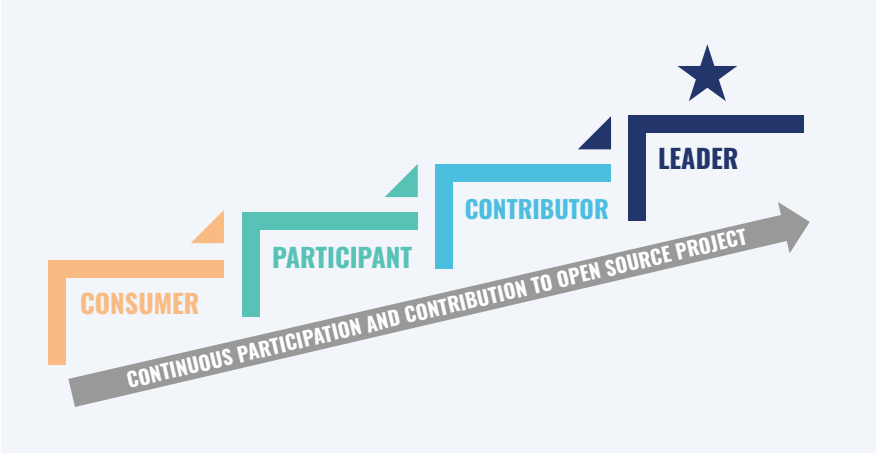
> NOTE: Maturity Models can be seen as a prescription for how OSPOs or open source engagement should develop. It can be tempting to think that it's always better to increase maturity. But, remember that you should consider what level of maturity is appropriate for your OSPO, or each function of your OSPO. Not every part needs to be highly developed. It may already deliver the value that's needed wihtout further development. If maturity models don't fit for your OSPO, consider using a capability model or something else that you prefer.

Example Maturity Models

Each of these maturity models is slightly different, but they all classify open source engagement from tactical and less intentional to strategic and more intentional.

Maturity Model 1 - Open Source Engagement Adoption by Dr. Ibrahim H[1]:

- Denial - No or unconscious use of open source
- Consumption / Usage - Passive use of OSS
- Participation - Engagement with open source communities
- Contribution - Pragmatic contributions to open source projects
- Leadership - Strategic involvement with open source to drive business value

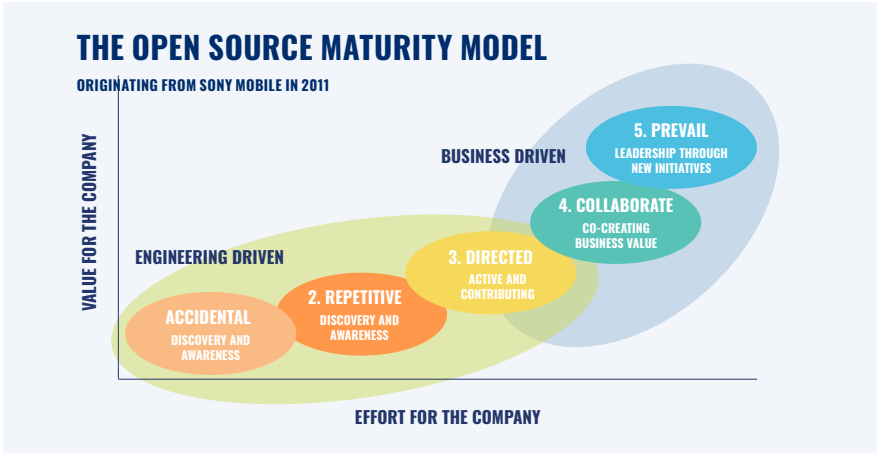


Maturity Model 2 - Five Stages of Corporate Open Source Adoption Talk by Carl-Eric[2]:

- Accidental - open source is used by the organisation without knowing that it's used
- Repetitive - there are processes set up for both consumption and contribution, but contributions are sporadic
- Directed - active participation incritical open source projects
- Collaborate - open source collaboration is used as a tool to create business value
- Prevail - open source is used to influence strategic areas of the business and technology

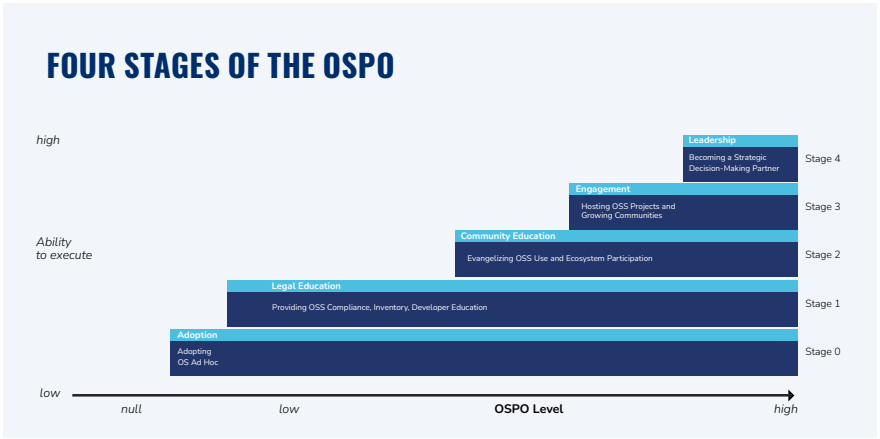
1 Dr. Ibrahim H, Guide to Enterprise Open Source: **https://www.linuxfoundation.org/research/guide-to-enterprise-open-source**

2 Carl-Eric: **https://web.archive.org/web/20240419100823/https://debricked.com/blog/what-is-open-source-maturity-model/**



Maturity Model 3 - The OSPO Maturity Model by The TODO Group[3]

- Stage 0: Adopting Open Source Ad Hoc
- Stage 1: Providing OSS Compliance, Inventory, and Developer Education
- Stage 2: Evangelizing OSS Use and Ecosystem Participation
- Stage 3: Hosting OSS Projects and Growing Communities
- Stage 4: Becoming a Strategic Decision-Making Partner



3 The TODO Group Maturity Model: **https://github.com/todogroup/ospology/blob/main/ospo-model/en/five-stage-OSPO-maturity-model.md**

Applying This to Your Organization

Here are some suggestions of how you could use the ideas and advice above to set up your OSPO. These are based on Maturity Model 3 - the OSPO Maturity Model by the TODO Group.

Using a Simple Checklist

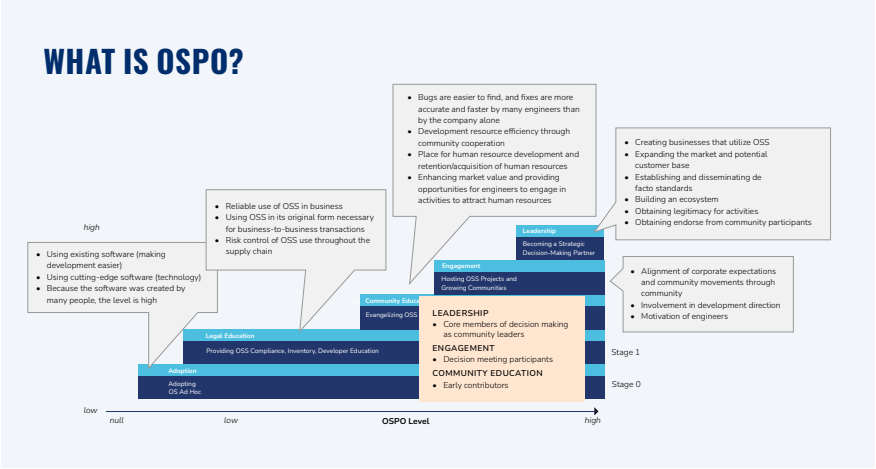
The TODO OSPO checklist[4] offers a simplified set of common milestones to both early-stage and seasoned OSPOs in navigating each stage of the previously mentioned OSPO maturity model. Please note that an OSPO might remove, add, or edit some content of this checklist to adapt it to their organization's needs.

Using Maturity Models

Once you have a certain familiarity with open source maturity models, you can start to use one to build your strategy and create your plan.

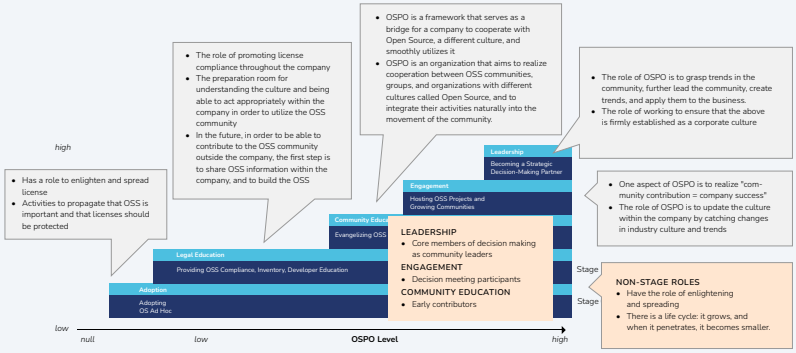
The OSPO Japan Local Meetup Working Group, supported by the TODO Group and OpenChain, has been developing a simple Frequently Asked Questions (FAQ) guide about OSPOs. This guide aims to answer questions at each step of the OSPO maturity model, which categorizes different open source activities from stage 0 to 4, and outlines the role of the OSPO at each level.

Here are some highlights from their work to inspire you:



4 The TODO OSPO checklist: **https://github.com/todogroup/ospology/blob/main/ospo-model/en/ospo-checklist.md**

WHAT ARE THE BENEFITS OF OSS ACTIVITIES?



> NOTE: You can find a summary of their work in both Japanese and English in a Qiita article written by one of its members[5]

While planning the OSPO it's very helpful have 1:1 conversations with managers, high-level executives, and workers/contractors from different teams that use open source in their day-to-day operations, or whose strategy involves dealing with open source projects (in terms of licenses, security vulnerabilities). Use the insights from these conversations to define the organization's unique motivators and map them to areas within the organization where open source brings value.

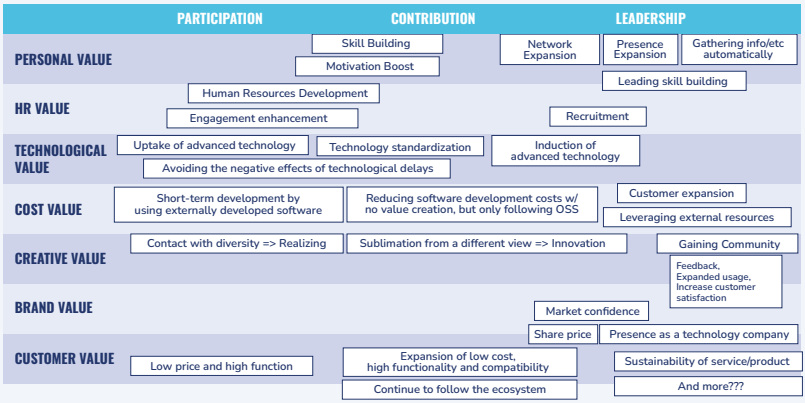
This will also help to build support for your work across the business even before the OSPO is officially created and launched.

Map these motivators with different activity types across the organization, by using the OSPO Maturity Model and creating a second division that categorizes each of these unique motivators according to the different stages. Use this as a reference when you are engaging and communicating with your stakeholders.

For example:

5 Summary of the work of The OSPO Japan Local Meetup Working Group in both Japanese and English in a Qiita article written by one of its members: **https://qiita.com/owada-k/items/017d1b98d0e437766bd0**

VALUE OF ACTIVITY FROM PARTICIPATION TO LEADERSHIP



Possible Problems and How To Overcome Them

PROBLEM	RECOMMENDATION
While creating the OSPO you are getting lots of questions and having to adapt your plan to take into account new information. It seems there is a lack of consistency in how open source understanding and value are perceived across the organization, leading to confusion and potential risks.	Ensure that you take the time to identify all your stakeholders and understand their motivations. Create publicly available open source manifestos, principles, and websites as an effective way to foster a common understanding of values, principles, and goals among all teams and subsidiaries. Taking time to establish and enforce a consistent understanding of open source throughout the organization will ensure a stable and strong foundation for the OSPO.

Resources

- TODO guide to outbound OSS: **https://todogroup.org/resources/guides/a-guide-to-outbound-open-source-software/**
- TODO guide to participating in open source communities: **https://todogroup.org/resources/guides/participating-in-open-source-communities/**
- DevOps uses Capability, not Maturity: **https://octopus.com/blog/devops-uses-capability-not-maturity**
- Porsche Open Source Website **https://opensource.porsche.com/**
- The Evolution of the OSPO **https://linuxfoundation.org/tools/the-evolution-of-the-open-source-program-office-ospo/**
- OSPO 101 training module - **OSPO and your organization: https://github.com/todogroup/ospo-career-path/tree/main/OSPO-101/module3**

CHAPTER 4: DAY-TO DAY OPERATIONS

Introduction

Once you have your strategy, you need a plan. Your plan will be to create and execute on a set of regular activities that deliver your strategy. This chapter will help you understand what the range of an OSPO's activities are, and what value each one delivers to your organization.

Common Activities

An OSPO's day-to-day operations encompass a broad spectrum of activities aimed at enhancing open source engagement and compliance within the organization, including:

- **Direct Open Source Support:** Involves answering questions on all aspects of open source, including license compliance, selecting OSS, and interactions with vendors. It also includes engaging with the community and partners, securing sponsorships, and organizing open source events.
- **Automation Tools:** Creating process automation to support open source policies is important because policies alone may not always be effective. Managers know that their workers won't always follow policy and therefore want effective options to automate use, management, and tracking of open source components. Automation is useful in many areas of open source including license compliance and security.
- **Documentation, Training, and Education:** An OSPO can play a leading role in ensuring that individuals are qualified to assess open source projects for use in the organization and contribute to critical open source projects for the organization. Developing training materials and documentation and/or aiding teams to produce these across different departments are key tasks.
- **Resource Allocation:** There can be a lot of areas that an OSPO can offer value to an organization. Therefore, prioritizing work and allocating resources strategically and tactically is an important activity that will improve the OSPO's impact.
- **Risk Management:** OSPOs are well-placed to take a holistic view of the risk that the organization faces when using open source projects. It's useful for the OSPO to assess the risks by obtaining a comprehensive view of the organization's tech stack. This may include generating SBOMs which allow the OSPO to consider the risks in software from vendors, legacy software, and proprietary software as well as in open

source. This is more about a business assessment perspective rather than just data gathering, as risk can only be managed, not eliminated. Optimizing SBOMs is about balancing risks against benefits.

- **Sponsoring Open Source Communities and Foundations:** Your organization depends on open source. The projects in open source are only as healthy as their communities, and you can invest your time and money in supporting communities either directly or through Foundations. These relationships need to be understood and managed with care to achieve outcomes that will benefit the projects and your organization. Sometimes money isn't the best fix for a problem, and fostering a closer partnership and providing development, marketing, or programmatic support is more useful.
- **Measuring Technical Debt:** Providing knowledge on how to measure the technical debt on an open source project helps to determine the risks associated with the project and, when done in collaboration with the project community, is a form of educational advocacy to help projects improve and sustain themselves.
- **Coordinating with Various Parts of the Organization:** It can be helpful to check that you know all your stakeholders, and have the right amount of interaction with them. Take a look at the OSPO flower diagram in Chapter 3 for help mapping interactions.
- **Giving Advice on Open Source Consumption:** The OSPO considers both the strategic view on which open source projects to consume and on the best practice for using the selected projects. The OSPO should provide reference materials and guidance on how the company should select which open source projects it uses and how it manages them. Guidelines and policy can be purely technical or can include considerations based on open source project health and practices, like the *Secure Supply Chain Consumption Framework (S2C2F)*[6].

Applying This to Your Organization

The OSPO MindMap

The OSPO MindMap[7] is once again a useful tool. You can use it to get an overview of the potential activities of an OSPO. The OSPO MindMap outlines the main responsibilities, roles, behaviors, and team sizes within the ecosystem of an OSPO. As always, this is an input to your work, not a fixed plan to follow. You should adapt it to your needs.

6 Secure Supply Chain Consumption Framework (S2C2F): **https://www.microsoft.com/en-us/securityengineering/opensource/osssscframeworkguide**

7 OSPO Mind Map **https://todogroup.org/resources/mindmap/**

Activities by Maturity Stage

In the following table, Ibrahim H.'s open source activity engagement model (previously seen in Chapter 2) is used as a map for listing and exploring activities in an OSPO.

STAGE: Consumer

ACTIVITIES	VALUE FOR THE OSPO	VALUE FOR THE ORGANIZATION
Define open source compliance rules and practices	An explicit consensus on the organization's open source compliance rules and practices between the legal and business stakeholders.	The organization knows that it has a managed approach to the legal aspects of open source consumption, which can be maintained and improved over time. Each company has different aspects of open source compliance, interpretations of licenses and different risk appetite (e.g dealing with regulations). Having well-defined compliance rules and practices is the first step toward deterministic open source compliance
Define rules and policies on using open source (criteria for using OSS which relate to open source health)	Consumption of open source projects isn't just viewed through the compliance lens, but is considered more holistically and includes the risks associated with unhealthy projects. A consensus is built in the company related to the hygiene of consumed open source components. The organization has clear policies to follow.	Consumed open source projects are lower in risk because they're healthy, fixing security vulnerabilities, implementing new features and release regularly.
Define rules and policies on how to contribute to open source (criteria on how to engage in the community, how to transfer rights, Contributor License Agreements)	The OSPO can increase awareness of the two-way relationship with open source projects. Using policies supports a consistent and ethical approach. The organization has clear policies to follow.	Policies and practices ensure that the organization considers how to jointly build value with open source projects. Contributions made are likely to improve the company's reputation, not damage it.
Adopt ISO/ IEC 5230 (OpenChain) Compliance	The OSPO can implement an international, defined standard rather than create one from the ground up.	The organization can demonstrate its compliance with an internationally recognized standard.

ACTIVITIES	VALUE FOR THE OSPO	VALUE FOR THE ORGANIZATION
Manage an inventory of OSS used in the organization	The OSPO is aware of the surface area of OSS it oversees.	The organization has a base for overall risk management. This is an important tool for dealing with issues relating to specific projects (security problems, license changes, lifecycle issues, etc.)
Training on open source awareness	Providing training on open source increases visibility of the role of open source, visibility of the OSPO and its value, and improves understanding of how the organization uses and engages with open source.	Increases the competence present in the organization to work with OSS through an awareness of open source value, licensing, and contributions etc.
Introduce tools for license compliance	Provide structure and visibility for licence compliance within the organization, which helps inform management strategy.	Automation is essential to be able to address risks with a reasonable amount of effort and measure effectiveness of efforts to improve compliance.
Clarify how to support OSS	Ensure that OSS is adopted with appropriate understanding of how it can be supported.	The organization should be aware of the hidden costs of using OSS in production scenarios. External support for open source components can sometimes be bought from a vendor or a service provider. Alternatively, other options are to manage the support yourself with the help of the community (being realistic in considering what a community can be expected to support), or going with the risk of not having support which may be appropriate for scenarios where the risk is low.

STAGE: Participant

ACTIVITIES	VALUE FOR THE OSPO	VALUE FOR THE ORGANIZATION
Financially supporting open source communities	Better relationships with communities, more influence.	Better stability in the ecosystem and software supply chain that the organization relies on.
Membership of open source organizations	Membership benefits such as co-marketing, event discounts.	Engagement with the communities the organization relies on. Potential influence and access to strategically useful information. Supporting the ecosystem.
Trying InnerSource	Staff in the organization will get hands-on experience with open source methodologies, which builds awareness, understanding, and advocacy.	The organization will build skills in its workforce that will contribute to better use of, and engagement with, open source projects.

STAGE: Contributor

ACTIVITIES	VALUE FOR THE OSPO	VALUE FOR THE ORGANIZATION
Create contribution policy and process	Managing open source contributions becomes easier.	Having clear procedures means that the organization can offer open source contributions in a legally safe way, for open source projects, the organization, and its employees.
Qualification of contributors	Contributors require less oversight and make good ambassadors.	Skilled contributors make better contributions into publicly-visible projects. This means less risk to the organization.

STAGE: Leadership

ACTIVITIES	VALUE FOR THE OSPO	VALUE FOR THE ORGANIZATION
Open sourcing previously proprietary projects	The OSPO can reduce the burden on the Engineering (and other) departments.	New opportunities will open up to improve the codebase of a commoditized component through collaboration in public. More strategic involvement in open source. Access to new expertise.
Establish an “upstream first” policy	Offering the organization a way to get more value for the same, or smaller, amount of effort.	The organization can support or even lead open source projects and make them part of the primary value creation of the organization without losing its competitive differences, and while benefiting from the contributions of a whole community.
Supporting autonomy of contributors and maintainers of open source projects	In-house experts in open source are valuable to the OSPO.	Employing people who are dedicated to only open source work means the organization can strategically strengthen important open source projects in the most organic and effective way.

Possible Problems and How to Overcome Them

PROBLEM	RECOMMENDATION
The new OSPO is very slow to make recognizable progress, and doubts about the need for an OSPO creep in.	As with all new ventures, it's really important to create and maintain a focus on delivering meaningful impact in the short and long term. Short term impact reassures stakeholders that the OSPO is needed and competent, and gives OSPO staff confidence. Long term impact creates sustainable value for the organization and embeds the OSPO securely in the organization. Try to identify something important that can be delivered within the first 3-6 months, while also working on longer term projects that will deliver in 6-12 months, 12-24 months and 2-5 years. Keep the list of active projects short at first to ensure that they're delivered with quality and on time. As confidence in the OSPO grows, it puts you in a stronger position to ask for more resource if you have a strong track record of delivering value.

Resources

- A Guide to Enterprise Open Source: **https://www.ibrahimatlinux.com/wp-content/uploads/2022/05/LFR_LFAID_Guide_to_Enterprise_Open_Source_052522.A4.pdf**
- A Deep Dive Into Open Source Program Offices: Structure, Roles, Responsibilities, and Challenges: **https://8112310.fs1.hubspotusercontent-na1.net/hubfs/8112310/LF%20Research/LFR_LFAID_Deep_Dive_Open_Source_Program_Offices_081922.pdf**
- OpenSSF Scorecard: **https://github.com/ossf/scorecard**
- Software Bill of Materials (SBOMs): **https://www.ntia.gov/SBOM**
- Computer Emergency Response Team (CERT): **https://www.cisa.gov/uscert/**

CHAPTER 5: MANAGING OPEN SOURCE SECURITY

Introduction

> NOTE: This chapter has been developed through the expertise of Open Source Security Foundation (OpenSSF) representatives, with support from the TODO Group

Open source software is an important part of the software supply chain. Because of this, it's part of an OSPO's responsibility to help secure the OSS supply chain. This includes tasks such as:

- Helping development teams assess the security of the OSS they use in products.
- Encouraging development teams to contribute to upstream open source projects to help improve their security.
- Following secure software development best practices in open source projects that the company maintains, contributes to, or leads.

This chapter includes useful resources to help OSPOs and open source developers apply secure software development and supply chain best practices - both in the software they use and the software they create.

In some ways, security is just like any other requirement. However, many software developers and their managers haven't received enough training in security. Also, security is about defending against intelligent attackers, and it often depends on how the entire system works together — not just on one part.

Fixing security problems later is often expensive. It's better to prevent them, reduce their chances or impact, and be prepared in case something still goes wrong. It's important to plan from the beginning and allocate resources (such as time and money) to handle security properly. Open source software can have a security advantage because it allows for mass peer review and follows the principle of "open design" — but these benefits don't happen automatically.

Training and Education

Many software developers and managers don't know what they need to know about security. This lack of knowledge often causes problems. Here are some key

areas to understand, along with links to free OpenSSF courses that can help. These specific courses aren't required, but it's important that everyone involved in software development gets the right training.

Managers (of both open and closed source projects) should understand how to manage secure software development. This includes knowing basic security terms, how to manage risks, how to build security into the design, how to protect all environments, how to identify risks early, and how to set clear expectations with stakeholders. Managers should also understand what their developers need to learn. If they haven't been trained yet, they can take the free Open Source Security Foundation OpenSSF course Security for Software Development Managers (LFD125)[1].

Developers should take a course on secure software development. This includes how to build secure software during planning, design, coding, testing, and release. Developers also need to know how to evaluate third-party software. They should understand common vulnerabilities (like those in the OWASP Top Ten for web apps[2] and CWE Top 25 for general software[3]) and how to avoid them. They should also know how to secure development environments and respond to vulnerability reports. If they haven't had this training, they can take the free OpenSSF course Developing Secure Software (LFD121)[4].

Both developers and managers must understand any laws or regulations they need to follow. For example, anyone involved in software that may be used in the European Union (EU) should understand the EU Cyber Resilience Act (CRA). This includes knowing what the CRA applies to, the different roles it defines (such as manufacturer or open source steward), and the legal responsibilities it creates. Because the CRA covers a wide range and includes strong penalties, those who need to understand it can take the free OpenSSF course Understanding the European Union (EU) Cyber Resilience Act (CRA) (LFEL1001)[5].

Key Steps

For developing your own software:

1. Review the OpenSSF Concise Guide for Developing More Secure Software, which links to practical resources[6].

---

1 Open Source Security Foundation OpenSSF course Security for Software Development Managers (LFD125) **https://training.linuxfoundation.org/training/security-for-software-development-managers-lfd125/.**

2 OWASP Top Ten for web apps: **https://owasp.org/www-project-top-ten/**

3 CWE Top 25 for general software: **https://cwe.mitre.org/top25/**

4 OpenSSF course Developing Secure Software (LFD121): **https://training.linuxfoundation.org/training/developing-secure-software-lfd121/**

5 **https://training.linuxfoundation.org/express-learning/understanding-the-eu-cyber-resilience-act-cra-lfel1001/**

6 Concise Guide for Developing More Secure Software: **https://best.openssf.org/Concise-Guide-for-Developing-**

2. Work to meet the OpenSSF Baseline, a short list of security checks[7].
3. Earn an OpenSSF Best Practices badge for your project. Start with "passing" and plan to achieve "silver" or "gold" over time[8].
4. Improve your OpenSSF Scorecard score. While this is often used to evaluate other projects, it can also help you measure your own[9].

Most modern software reuses other software. Choose and use open source components carefully:

- Use the Concise Guide for Evaluating Open Source Software[10].
- Double-check software names to avoid "typosquatting" attacks (where malicious packages have names similar to trusted ones).
- Use the OpenSSF Scorecard to evaluate software before using it[9].

Protect your environments, including development, build, test, and distribution:

- Use multi-factor authentication (MFA) to make it harder for attackers to gain access.
- Secure your build environment. See OpenSSF SLSA for more guidance[11].

Use automated tools in your continuous integration (CI) pipeline to catch security issues early:

1. Use multiple types of tools, as each may find different problems, see the Guide to Security Tools[12].
2. For new projects ("green field"), enable all security checks. For older projects ("brown field"), start with the most important checks so the reports are manageable
3. Enable tools that detect known vulnerabilities in reused components

Prepare for vulnerability reports — they can happen to any project. Clearly explain how people can report vulnerabilities. Open source projects should review the OpenSSF Guide to implementing a coordinated vulnerability disclosure process[13].

More-Secure-Software

7 **https://baseline.openssf.org/**

8 OpenSSF Best Practices badge **https://www.bestpractices.dev/**

9 OpenSSF Scorecard: **https://github.com/ossf/scorecard**

10 Concise Guide for Evaluating Open Source Software: **https://best.openssf.org/Concise-Guide-for-Evaluating-Open-Source-Software**

11 OpenSSF SLSA: **https://slsa.dev/**

12 Guide to Security Tools: **https://github.com/ossf/wg-security-tooling/blob/main/guide.md#readme**

13 OpenSSF Guide to implementing a coordinated vulnerability disclosure process: **https://github.com/ossf/oss-vulnerability-guide/blob/main/maintainer-guide.md#readme**

Applying This to Your Organization

Improving the security of OSS in your organization isn't just about using tools. It also requires changes in culture and daily work processes. One of the first steps is to build a mindset where security is everyone's responsibility, not just the job of a small team. Leaders should clearly communicate that secure software development is important and support this with time, resources, and recognition for those who work on it.

Security practices should be part of everyday development work, not something separate. For example, instead of running security checks only once in a while, make tools like scorecards and vulnerability scans part of your regular CI/CD pipeline. This helps make security a normal and expected part of how your team builds software.

Training and education should happen regularly, not just once. Developers and managers should be encouraged to learn the basics of secure software development. This can include free OpenSSF courses and other programs. Make sure your teams know that learning about security is important and will be recognized. This builds long-term interest and responsibility.

It also helps to be open about security progress. Encourage teams to track and share their progress on goals like earning Best Practices badges or improving their Scorecard results. This creates a positive environment where teams help each other and improve together, instead of feeling blamed when something goes wrong.

Lastly, support continuous improvement. Security isn't something you finish — it's always changing. Set up regular times to review risks, update tools and practices, and share what your teams have learned. Give teams the freedom to make decisions about security early in the development process, not just at the end or after a problem happens.

By creating a culture of shared responsibility, adding security into everyday work, investing in learning, encouraging openness, and improving over time, your organization can make real progress in securing the OSS it builds and uses.

Resources

- OpenSSF: **https://openssf.org**
- OWASP: **https://owasp.org/**
- CWE: **https://cwe.mitre.org/index.html**

CHAPTER 6: USING METRICS IN YOUR OSPO

Introduction

> NOTE: This chapter has been developed through the collective expertise of CHAOSS open source project and participants from the CHAOSS OSPO Metrics Working Group, with support from the TODO Group.

Metrics are an important part of any modern organization. When used effectively, they offer a valuable way to track the impact of your team and its projects. For an OSPO, metrics not only support planning and measuring the impact of its work — they also provide deeper insight into the open source projects the organization depends on.

In the past, it might have been acceptable to know little about key open source projects. But that's no longer a sustainable approach as the regulatory and security landscape around open source continues to evolve. As we deepen our understanding of the open source projects that matter to us, community metrics become essential tools. In this chapter, we'll explore how to place those metrics in context and how, together, they can offer better insights to guide strategic decisions across an organization.

There are several reasons why organizations need visibility into open source projects. For example:

- The organization is using open source and wants to track contributions to key projects.
- The organization participates in an open source ecosystem and needs to identify potential risks and offer support where necessary.
- The organization wants to contribute to the sustainability of OSS — especially the software that's critical to its business.
- The organization must stay compliant with upstream license requirements and respond to security issues that could affect operations.

The Goal-Question-Metric Framework

Metrics for metrics' sake benefit no one. Consider these metrics:

- The average age of issues is 10.3 days.
- The total number of pull requests was 121 last month.
- We had 3 new companies join our community over the past 15 days.

Without context, these metrics provide no insight, so it's important to ensure that you use a framework like "goal-question-metric" to give you metrics that support your goals instead of working against them.

The CHAOSS project (Community Health Analytics for OSS) advocates for using the "goal-question-metric" because it's a structured method for deriving metrics that align with organizational goals. It involves three key steps:

Goals

Identify and understand your organizational goals. These can vary significantly but typically include objectives like recruiting talent or enhancing community engagement.

Questions

Break down these goals into specific, actionable questions. For example, to assess recruitment efforts, one might ask, "Who are important contributors?" or "How many did we help hire?"

Metrics

Develop metrics to answer these questions. Metrics should be operational and data-driven, such as the number of contributions by name, hiring successes, or project activity levels. Some good data points, like the number of commits (on a software project), may not be relevant to the question you need to answer.

Understanding the Role of Open Source Community Metrics

It's worth taking a moment to understand how open source community metrics support the other types of metrics that organizations are familiar with. Open source community metrics provide OSPOs with tangible ways to measure the influence, effectiveness, and strategic value of their open source initiatives.

By tracking contributions, engagement levels, and collaboration across projects, OSPOs

can assess how well their organization is participating in and supporting the open source ecosystem.

These metrics help demonstrate the impact of open source work on broader business goals such as accelerating innovation, reducing development costs, attracting talent, and increasing product visibility. Metrics also provide insight into community health and sustainability, highlighting whether a project is gaining traction, fostering collaboration, and attracting active users and contributors.

By tying community metrics to organizational KPIs, OSPOs can showcase the value of open source beyond code, such as improved product feedback loops, faster time to market, stronger developer relations, and enhanced technical credibility. This playbook provides guidance for OSPOs to track, analyze, and communicate those metrics effectively, translating open source participation into measurable business impact.

Using Metrics to Communicate the Impact of Your OSPO

Metrics play an important role in communicating impact. Following the goal-question-metric approach here are four goals that OSPOs can consider, and questions to go with them.

1: Partner Impact

Goal

Understand how open source collaboration fosters strategic partnerships that can enhance market insight, strengthen vendor relationships, and create shared value beyond individual technologies.

Commentary

Open source project work is premised on collaboration, a collaboration that often involves unexpected partnerships. These partnerships are aimed at developing non-differentiating technologies that each partner needs, yet doesn't necessarily have the resources or inclination to produce alone. Open source projects bring together organization members to work together in the pursuit of shared problems and this proximity can result in benefits beyond any one shared open source technology. Improved open source partnerships can have positive secondary effects, including stronger ties with upstream vendors, improved understanding of market rival positions, and direct interaction with downstream users.

Questions

- What other companies are involved in our open source projects of interest?
- What other companies are involved in our pull requests?
- How are other companies involved in our pull requests?
- What's the composition of involved companies as our vendors, rivals, and customers?

Metrics

Consider what data is available to you to be able to answer these questions, and what other information you would need to feel confident in what it would mean to your goals if the number goes up or down.

2: Community Impact

Goal

Evaluate how employee engagement in open source communities reflects organizational support, strengthens individual skill development, and enhances the organization's presence and influence in key projects.

Commentary

There are ways that an organization can support community engagement by employees (for example contribution guidelines, intellectual property management, and license support). Support will often include why the community is important to your organization - including a time and prioritization component in how much time an employee spends in external/upstream work. companies can observe employees as good citizens for reasons of personal and organizational gain, and help employees understand their importance in bridging between the organization and the community.

Questions

- What percentage of employee contributions are merged?
- What percentage of employee issues are closed without conversation?
- How many of our employees have maintainer or leadership roles in key open source projects?
- Have upstream contributions helped modernize tech skills for employees?
- Which projects do our employees make over 50% of the contributions?

Metrics

Consider what data is available to you to be able to answer these questions, and what other information you would need to feel confident in what it would mean to your goals if the number goes up or down.

3: Ecosystem Impact

Goal

Monitor and contribute to the health and resilience of open source ecosystems to ensure long-term viability, reduce risk, and support the strategic sustainability of key dependencies.

Commentary

Working with open source is never easy as rival corporations may dominate upstream projects that your organization is interested in, upstream projects may unexpectedly change licenses, and contributor agreements, whether individual or organizational, can be complex to understand and adhere to. Clearly, such challenges can be overcome and often include strategic engagement with the projects your organization aims to benefit

from. Open source ecosystems are economic and social systems comprising different companies, motivations, and requirements intended to support production and demands. In an effort to ensure the efficiency and durability of any open source ecosystem, companies must not only monitor the ecosystem's long-term viability but also engage within the ecosystem when problems are identified and stabilization is required.

Questions

- What percentage of our suppliers provide OSS bills of material?
- What's the long-term viability of the open source projects we rely on?
- What's the risk to the ecosystem if an open source project becomes unviable?

Metrics

Consider what data is available to you to be able to answer these questions, and what other information you would need to feel confident in what it would mean to your goals if the number goes up or down.

4: Organizational Impact

Goal

Align open source engagement with internal governance, security, and product development to maximize the value of open source within organizational strategy and operations.

Commentary

Engagement with open source communities includes working in the upstream to effectively use OSS in organizational products. In this, there is a need to monitor the intake of OSS for infosec, legal, and engineering reasons. Companies can establish software intake processes, working with teams to either technically track or socially consider issues related to open source intake. Organizational impact can also include working downstream with projects and companies that rely on your organizational products. This can include working to gain a clearer picture of the open source that is in your shipped products. Organizations can work in securing and regulating their own internal open source processes in an effort to improve product development activities.

Questions

- What characteristics does an organization inspect related to inbound OSS?
- What product-level software and infrastructure contains OSS dependencies?
- How is OSPO strategy aligned with organizational strategy and departmental objectives?
- How often is OSPO strategy used to guide business decision making processes?
- How does the use of open source influence organizational value?

Metrics

Consider what data is available to you to be able to answer these questions, and what other information you would need to feel confident in what it would mean to your goals if the number goes up or down.

If You Manage Open Source Projects

For organizations that create and manage their own open source projects, or are closely involved in managing them, there is a series of metric-related CHAOSS Practitioner Guides[1] to guide you through identifying the right metrics for a selection of use cases.

If You Use Open Source Projects

For organizations that use open source projects and want to understand the health of these projects, the following information can help them consider what's right for them.

How OSPOs Can Navigate the Complexities of Open Source Project Health

Understanding the health of an open source project is not a simple task. Open source health includes many different concerns—both technical and social—that can appear at the project level or across the broader ecosystem. A review of existing research identified 107 such concerns[2]. To help make sense of this complexity, researchers worked with 17 experts from industry and the open source community to organize these concerns into a framework of 21 health aspects.

---

1 CHAOSS Practitioner Guides: **https://chaoss.community/about-chaoss-practitioner-guides**.

2 Linåker, J., Papatheocharous, E., & Olsson, T. (2022). How to Characterize the health of an Open Source Software project? A snowball literature review of an emerging practice. In the 18th International Symposium on Open Collaboration. DOI. **https://doi.org/10.1145/3555051.3555067**

- These health aspects focus on important areas such as:
- Community productivity and stability.
- Project orchestration and leadership.
- Production processes and outputs.

Each health aspect is further described using attributes—smaller, more detailed elements—that help organizations examine project health in a structured way.

Matching the Framework to the Right Context

The experts interviewed emphasized that organizations must consider the type and characteristics of each open source project they're analyzing. Not all projects are the same, and different traits may influence how to assess their health. Important factors to look at include:

- The life cycle stage of the project (for example early stage vs. mature).
- Its complexity (how big and technically demanding it is).
- The governance model (how decisions are made and who makes them).
- The strategic value the project holds for the organization

When comparing open source projects, OSPOs should group and assess projects with similar characteristics. Comparing very different types of projects can lead to misleading results[3].

Making Smart Choices About What to Measure

Every organization has a different context—different markets, technologies, and risks. Because of this, there is no "one size fits all" approach to assessing open source health. OSPOs should:

- Decide which health aspects and attributes matter most based on their organization's needs.
- Prioritize efforts — it's too time-consuming and expensive to measure everything.
- Focus on the data that provides the most useful insights for risk management and decision-making.

Instead of trying to measure everything at once, OSPOs should start small, learn from early efforts, and refine their approach over time. Health assessments work best when

3 Lumbard, K., Germonprez, M., & Goggins, S. (2023). An Empirical Investigation of Social Comparison and Open Source Community Health, Information Systems Journal, 34(2), 499-532. **https://onlinelibrary.wiley.com/doi/abs/10.1111/isj.12485**

OSPO END-USER JOURNEYS

The OSPO End User Journey report highlights active Open Source Program Offices Practitioners and demonstrates how their organizations grow their open source knowledge and benefit from building a strategic vision and commitment around open source through an OSPO.

Use cases will be added as more organizations contribute to expanding this list.

- **Porsche End-User Journey Report**[1] Use-case
- **Sony End-User Journey Report**[2] Use-case

Porsche End-User Journey Report Use-case

Sony End-User Journey Report Use-case

1 https://github.com/todogroup/ospology/files/14300430/Porsche-enduser-OSPOCaseStudy.pdf

2 https://github.com/todogroup/ospology/files/13006962/sony_end-user-OSPOCaseStudy.pdf