WHITEPAPER

The Rise of the Open Source Program Office

FOSSA

TL;DR

Open source programs are an emerging and critical part of a company's software strategy. Industry leaders in tech like Microsoft, Google, Twitter and Netflix, as well as industry leaders in more established industries like Samsung, Comcast, and Intel have all established open source program o!ces (OSPOs). Outside of these giants, over 50% of "large" companies across tech, consumer electronics, financial services and telecom are establishing or planning to create an OSPO.

The key pillars of a successful OSPO are:

- **COMPLY**
  Be a responsible member of the open source community.
- **CONTRIBUTE**
  Build in a process for your engineering team to contribute to current open source projects.
- **CARE**
  Give back to the community, whether it is through publishing open source projects, sponsoring open source developers, or hosting open source events.

A Guide to Getting Started

Managing your open source program is all about improving efficiency and decreasing risk. Determining what packages to leverage, when developers should contribute, and what internal projects you may want to publish are all strategic business decisions. The decisions around open source usage and contribution should be a part of broader strategic company decisions. Determining factors such as which open source licenses are appropriate, whether or not your full-time employees should be contributing to a major open source project, and determining what components will best accelerate your products growth, quality, or security all have implications on both your product's viability and competitiveness, how your internal resources are being used, and what the risk profile of your company is.

> "We seek to create a working environment that talent wants to be part of. Our engineers know that they work in an open source-friendly environment where they are supported and encouraged to work with the open source communities that are relevant to their work."

Gil Yahuda | Verizon Media's OSPO Leader

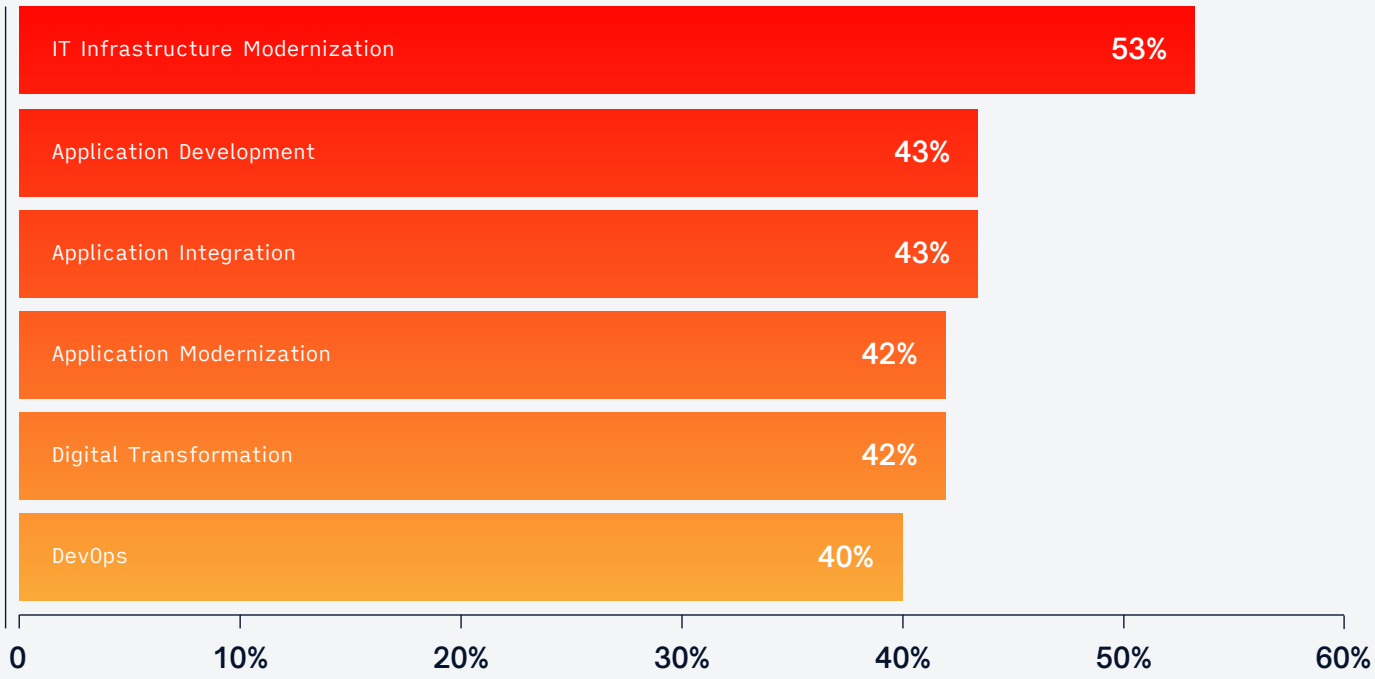
What is an OSPO?

Open source software is fundamentally different from proprietary software. Sometimes open source is owned by internal employees, sometimes it's not. Sometimes your company has influence over the roadmap, sometimes not. Often, different teams use and / or build open source differently. Because of this variability, it needs to be approached differently. Managing this strategy is the job of the OSPO (Open Source Program Office).

What does an OSPO manage?

1. **Oversight of open source package selection,** based on both usage and licensing requirements, for use in development
2. **Enablement for development acceleration** based on open source usage in order to meet business goals
3. **Oversight of corporate risk profile** against open source license compliance and release schedules
4. **Stewardship of corporate open source ethics** and "good citizenship" within the open source community including contributions back to the community

What is Enterprise Open Source Being Used for?



Source: “The State Of Enterprise Open Source - Redhat.com.” Enterprise Open Source Report 2019, RedHat 15 Apr. 2019, www.redhat.com/cms/managed-files/rh-enterprise-open-source-ebook-f16984bf-201904-en_1.pdf.s.

How do you Get Started?

Set an Initial Goal

Determine what priority aligns most with company goals. For many companies, getting started means coverage against risk associated with open source compliance and / or open source security. For others,

the number one priority might be launching an open source project or recruiting top open source talent. This is variable based on processes already in place and your company's overarching initiatives.

Once you have your goal, determine initial success criteria. Examples include:

- Mandate to decrease compliance risk for internal products
- Improving the ratio of internal to external contributors to your open source project as a demonstration of market adoption
- Targeting a number of external adopters for your open source project
- Developing a recruiting goal around open source talent and leveraging your reputation in the open source community

"Good open source policies include legal counsel on which open source licenses are permissible for each company product. How to contribute to existing open source products, and which licenses should be utilized when publshing internal products to the open source community."

Find the Right People

The OSPO is typically sta"ed with personnel from multiple depart- ments within the company, and

should not strictly be the domain of the development team. It should include one or more of the following roles:

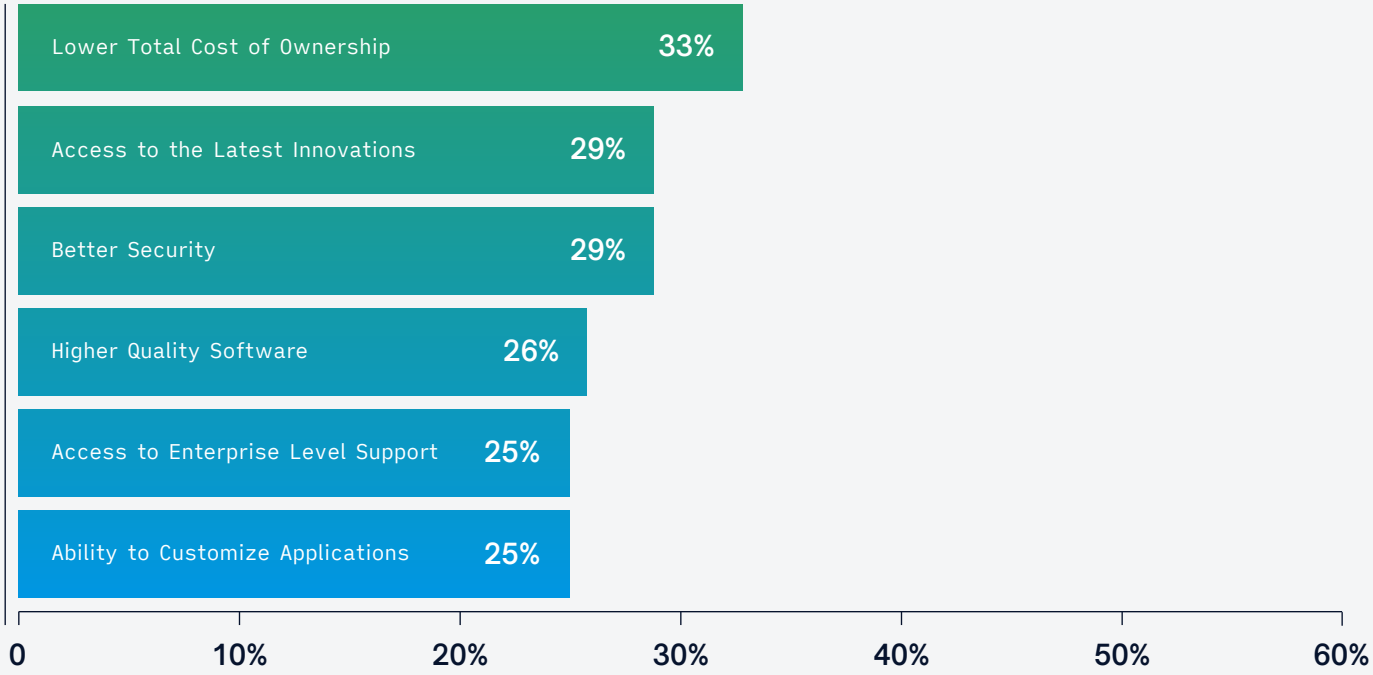
- **Program Manager**
  It should be this person's full-time responsibility to quarterback all program initiatives, advocate for resources, and help manage the strategy for open source at your company. They should dictate how open source strategy aligns with your overarching business goals from revenue targets, to recruiting efforts, to brand awareness, to engineering excellence.

- **Legal Support**
  While it is near impossible to embrace modern development practices without adopting open source software, leveraging open source technologies does not come without risk. Open source licenses should be viewed similarly to patent or copyright law. Each license includes instructions on how open source components can be used and the additional obligations that are required in order to adhere to the license. A failure to comply can result in missed business opportunity or loss of revenue (failed acquisitions or IPO challenges, or sales that are lost due to open source compliance requirements), legal actions (loss of IP ownership, damage to reputation which could have revenue or partnership impacts, fines, etc.), and damaged

engineering brand which could negatively impact recruitment efforts in competitive areas.
Good open source policies include legal counsel on which open source licenses are permissible for each company product, how to (or whether to) contribute to existing open source products, and which licenses should be utilized when publishing internal products to the open source community.

- **Product and Engineering Support**
  The role that product and engineering plays in an OSPO varies from company to company, depending on company size and team structure. First and foremost, there needs to be product / engineering buy-in for any processes, systems, and strategies. Without that, your program is unlikely to succeed. In some companies, an OSPO will even have an engineering team owning any open source contributions.
- **IT**
  From DevOps to Security, having support from the IT department is key. An OSPO may be tasked with implementing internal tools to improve developer e!ciency, monitor open source compliance, or dictate open source security measures. IT is key in helping to connect workflows, and ensure policies are implemented in a developer-friendly manner.

Top Benefits of Using Enterprise Open Source Solutions and Technologies



Source: “The State Of Enterprise Open Source - Redhat.com.” Enterprise Open Source Report 2019, RedHat 15 Apr. 2019, www.redhat.com/cms/managed-files/rh-enterprise-open-source-ebook-f16984bf-201904-en_1.pdf.s.

Executive Sponsor

For any program to get the resources it needs to be successful, executive buy-in is critical. Depending on your first initiative, this executive sponsorship can lie in several different roles:

- **VP Engineering and CTO**
  Open source initiatives frequently map to engineering excellence. Not only does having a strong open source program improve software developments (building towards any engineering excel- lence initiatives), but strong open source programs often attract great engineering talent.

- **CIO**
  Open source initiatives also have strong ties to IT initiatives, from developer e!ciency to modernization efforts. A recent survey found that 53% of Enterprise IT leaders are using open source to modernize IT infrastructure, 42% are using open source for digital transformation efforts and 40% are using open source software for DevOps[1]. Finding a way to streamline usage, governance, and adoption of open source is key to the success of many IT teams.

- **Compliance & Risk**
  For many companies, the first initiative under an open source program is to ensure open source compliance and limit a company's risk exposure. This falls squarely under a Chief Compliance Officer's mandate.

1 "The State Of Enterprise Open Source - Redhat.com." Enterprise Open Source Report 2019, RedHat 15 Apr. 2019, www.redhat.com/cms/managed-files/rh-enterprise-open-source-ebook-f16984bf-201904-en_1.pdf.

Key Pillars of a Successful OSPO

There are three key pillars to successfully run OSPOs: comply, commit code, and contribute.

Comply

Be a responsible member of the open source community. Use open source components in adherence with their respective licenses. Not only does this ensure you are in good standing with the open source community and improve your brand reputation, but this is also key to limiting your company's risk profile.

Contribute

Build in a process for your engineering team to contribute to current open source projects. There are several legal policies around copyright and intellectual property that dictate a clear policy be in place before your engineers can contribute to existing open source projects.

Care

Give back to the community, whether it is through publishing open source projects, sponsoring open source developers, or hosting open source events. There is no right way to give back to the community, so figure out what aligns with your business strategy.

“Although each company is different, these recommendations are based on discussions with industry experts, OSPO leaders, and observations around successfully implemented entereprise open source programs.”

Key Pillars of a Successful OSPO

Compliance

Although each company is different, open source compliance is key for everyone. Open source compliance can dictate what companies you can sell to or partner with, what your company valuation is in a merger or acquisition (high risk means lower valuation), and what exposure you have to potential litigation or reputation damage. For most companies, tackling compliance is (and should be) the first mandate of an OSPO. Open source compliance is also a more concrete and actionable initiative and is great for establishing early OSPO wins.

In order to become a responsible consumer of open source you need to develop an understanding of open source licenses—we recommend perusing tldrlegal.com or reading Open Source for Business: A Practical Guide to Open Source Licensing by Heather Meeker. Leveraging this understanding of the intricacies of various licenses, create policies around which licenses are appropriate for different projects.

Licensing is extremely nuanced and different licenses are often permissible for one company project, but not another.

For advice on developing policies, read or listen to Kate Downings talk on developing a comprehensive third-party package policy.

Once you understand what types of open source are permissible, you need to understand what open source your company is using.

Rather than a manual approach, we recommend leveraging an open source management tool that can automate generating lists of open source dependencies. Since modern software development practic- es promote CI / CD (continuous integration, continuous delivery / continuous deployment), ensuring your lists are continuously updated with new code commits is crucial to maintain compliance.

Finally, develop processes to ensure your open source dependencies are compliant. This is frequently the most difficult part. You will want to ensure the processes you develop are e!cient, scalable, and automated. Key areas to focus on when developing a system are minimizing developer workflow interruptions, minimizing manual resolutions, and streamlining communications across the teams involved (generally IT, engineering, and legal).

Though many companies start this process by leveraging spread- sheets and manually tracking down dependencies, it is better to leverage software

(such as FOSSA) in order to improve both efficiency and accuracy.

> **“When you contribute to a project with enhancements, your contributions are likely to be included in future versions of the open source project. Futhermore, your contributions may be extended by extremely talented engineers across multiple organizations.”**

Contribute

Contribution is a core pillar of the open source community mindset. However, the extent to which a company contributes varies. It is up to your OSPO to determine the correct strategy for your company. No matter the extent of contribution, it is valuable to have painless processes in place for engineers to contribute.

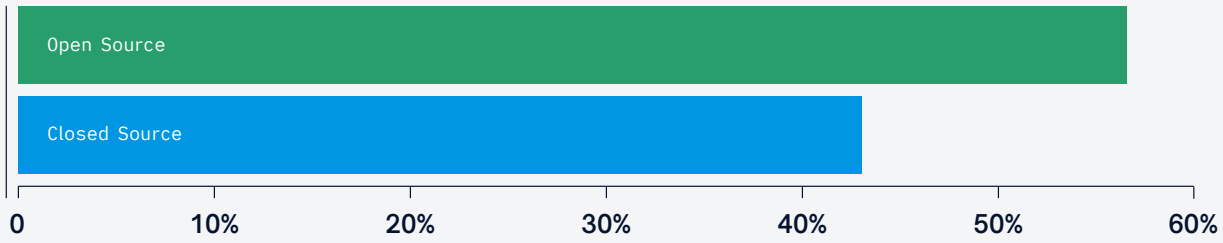
Building strong processes that empower your engineers to contribute code is important for two main reasons. First, your engineering team may need to contribute or adapt open source projects in order to successfully integrate them into proprietary software. A great example of this is FOSSA’s CLI. Because it is open source, engineering teams are able to contribute in order to ensure it easily integrates into their own build systems.

Contributing is also a way to help future-proof

your decision to leverage specific open source components. When you contribute to a project with enhancements, your contributions are likely to be included in future versions of the open source project. Furthermore, your contributions may be extended by extremely talented engineers across multiple organizations. Second, and almost more importantly, top engineering talent is drawn to companies with strong open source programs[1].

“Smart developers are drawn to smart code - which is visible if it’s open sourced.”

Most Applied-to US Tech Startups



Source: AngelList. “Want To Recruit Better Engineers? Open Source Your Code.” AngelList, AngelList, 19 Nov. 2018, angel.co/blog/want-to-recruit-better-engineers-open-source-your-code.

1 AngelList. “Want To Recruit Better Engineers? Open Source Your Code.” AngelList, AngelList, 19 Nov. 2018, angel.co/blog/want-to-recruit-better-engineers-open-source-your-code.

Smart developers are drawn to smart code—which is visible if it is open sourced. Of the top 30 tech companies, over half of them have open source programs. This is best stated by Gil Yahuda, Verizon Media's OSPO leader ... "We seek to create a working environment that talent wants to be part of. Our engineers know that they work in an open source friendly environment where they are supported and encouraged to work with the open source communities that are relevant to their work."[1]

Ensuring your contribution process is easy and painless is crucial for engineering adoption. There are several resources available for de- veloping internal policies. Google's guides are all publically available here. We recommend working with open source lawyers to create policies in order to ensure you are not publishing proprietary code.

Care

Finally, establish a means of giving back to the community. Whether or not this means developing your open source project depends on your business, but finding strategic ways to support the community is highly leveraged for both recruiting and ensuring popular projects you rely on have the support and resources they need to be maintained. Some examples of ways companies have given back to the community are publishing guides and stories of their success creating open source management

1 "Recruiting Open Source Developers." The Linux Foundation www.linuxfoundation.org/resources/open-source-guides/recruiting-open-source-developers/

programs, sponsoring events for open source projects, and donating to open source projects.

Further Reading

Learn from Open Source experts

- **TODO Group**
  https://todogroup.org/guides/
- **The Linux Foundation**
  https://www.linuxfoundation.org/resources/open-source-guides/
- **CNFC**
  https://www.cncf.io/

Learn from the Enterprise

- **Google**
  https://opensource.google.com/
- **Microsoft (GitHub)**
  https://opensource.guide/
- **Facebook**
  https://code.fb.com/category/open-source/