BLACKDUCK

BearingPoint®

OPEN SOURCE GOVERNANCE IN HIGHLY REGULATED COMPANIES

Open source software (OSS) can empower developers, increase innovation and improve competitiveness, and its popularity is growing tremendously. Open source now represents an average of 29 percent of the code deployed by IT, and technology innovators are using 60 to 80 percent of open source code, which can yield cost savings and free-up development resources to improve competitive differentiation. And as open source becomes more common, the need for governance increases dramatically. Without proper controls and processes to ensure compliance and reduce exposure, organizations will be at risk from technical and operational, regulatory, security, legal and brand factors. It is more important than ever to ensure developers use approved and supported code.

INTRODUCTION

Open source governance is part of IT governance and focuses on the specific issues related to the acquisition, use and management of OSS, and ensuring it is done in alignment with a company's stated objectives, policies and risk profile.

In many companies, the use of open source components in IT application development has historically been forbidden, largely uncontrolled or both, but that has not prevented it from being widely used and deployed. Developers enjoy the freedom and creativity of leveraging the abundance of open source code available on the Internet, often without a formal acquisition process. In fact, even with tepid management support, open source has reached a tipping point: in January 2011, Gartner surveyed 547 IT leaders and reported that software deployed by IT organizations has an equal amount of open source and internally developed code. Technology innovators are using 60 to 80 percent open source in their code[1], and as they realize significantly more benefit from the code, adoption increases.

The difference in open source use represents a large potential reduction of development investment that could be realized as cost savings, but more typically, customers shift that potential – with flat or declining development budgets – to areas that create competitive value. In addition to internal use of open source, most outsource development organizations thrive on the use of open source code, which creates additional entry points and increases the complexity and exposure for Enterprises.

Since open source has traditionally been uncontrolled despite it wide use and deployment, the need for management, visibility and control has grown to the point where formal governance processes are required. Mark Driver, Gartner's lead analyst on open source, recently reflected on this development: "Open source is ubiquitous, it's unavoidable…having a policy against open source is impractical and places you at a competitive disadvantage." In fact, Gartner predicts that "by 2014, 50 percent of Global 2000 organizations will experience technology, cost and security challenges through a lack of open source governance." The urgency is growing for management to catch up with the reality of how software is built today.

OPEN SOURCE: MAXIMIZE THE RETURN WHILE MINIMIZING THE RISKS

The benefits of using open source are well-known and widely reported, and include reduced cost, increased IT flexibility and innovation and faster time-to-solution. According to Jeff Hammond, principal analyst at Forrester Research, open source is a "silver bullet" that allows simultaneous improvement along all three dimensions of the software "iron triangle" of cost, schedule and features. However, the uncontrolled use of open source and the lack of formal acquisition processes can expose an organization to material risks.

1. Based on Black Duck's experience with nearly 1,000 customers

Unaudited and unmanaged open source technology proliferates with an enterprise software portfolio and is hidden as a ticking time bomb that eventually results in technical failure that cannot be sufficiently addressed, security risks that can result in a significant loss of business value, and potential intellectual property (IP) risks that can result in legal action.

– Gartner

Risks from the use of open source include:

- Technical and operational
- Regulatory
- Security
- Legal
- Brand

TECHNICAL AND OPERATIONAL

The technical and operational risk from the uncontrolled use of open source manifest in a number of areas, including:

- Code quality/integrity
- Ability to obtain support
- Viability of the community behind the open source project

While a number of popular open source projects are reported to be of higher quality than commercial code, there are over half a million open source projects available on the Internet, and quality is not uniform. There are often multiple open source alternatives to choose from, which adds to the complexity of decision making and the need for tools and data to assist in the process. Open source code needs to be tested and vetted like other software.

When open source is used in mission critical operations, a clear plan and path from the code to where it's used to how and where to obtain support and fixes are critical. The issue of where to and how to obtain support for open source projects is a topic of frequent discussion – for example, buying commercial support versus relying on the open source community versus providing self-support.

Operational risk can also develop from too much reliance on a particular project. Many IT organizations rely on the community behind a project for support and enhancements, often becoming part of the community themselves. A development team may inadvertently create risk and exposure by choosing a project that becomes stagnant or dies. Questions that should be addressed when a component is chosen include:

- If a problem arises with the code, who will fix it?
- Is the community behind the project viable and robust?
- Will the project continue to grow and thrive?
- How will we support it?
- Should we contribute back to the community?

REGULATORY

Regulatory compliance is concerned with meeting the obligations of regulations that may be affected by the use of open source, which include, but are not limited to: Sarbanes-Oxley, Basel II and III, data privacy regulations and export regulations.

Open source is often integral to how users and applications interact with critical business data. The lack of visibility on what the code is doing and how it works can represent a major control oversight of the data and create regulatory exposure. In addition, the way developers integrate open source with proprietary code can affect IP ownership. For example, in March 2011, a former Goldman Sachs programmer received an eight-year jail term for theft of intellectual property in the form of software. The programmer originally claimed he inadvertently mishandled open source code and Goldman's proprietary code for one of its major trading platforms.

SARBANES-OXLEY ACT

Sarbanes-Oxley requires verification of the ownership of material assets, and brings personal accountability directly to corporate managers. Section 302 "Disclosure Controls" requires reporting of any material weakness of internal controls. Section 404 "Assessment of Internal Controls" requires a management assessment of the effectiveness of internal control structure and procedures. As open source has grown in popularity and awareness, knowledge of the lack of controls around its use and the commensurate implications are growing as well. Improper vetting of open source acquired by developers, lack of oversight to comply with the legal obligations and ignorance of vulnerabilities in open source code are all areas where automation tools and best practices are available to minimize and control the risks.

BASEL II AND III

In Europe, the Basel II framework (and the forthcoming Basel III framework with general effective date of 2013), specifies how much capital banks need to put aside to guard against the types of financial and operational risks that banks face. The Goldman Sachs example referenced above highlights how the lack of operational controls over code can directly create risk and exposure.

DATA PRIVACY REGULATIONS

There are a growing number of data privacy regulations that reinforce the need to manage potential exposure from the use of external code.

The Payment Card Industry Data Security Standard (PCI) is an information security standard for organizations that handles cardholder information. It requires the protection of cardholder data and requires an annual validation of compliance, including the requirements that organizations maintain secure systems and applications, have strong access control, monitor and test access, as well as maintain a policy that addresses information security. Again, the lack of operational controls around the acquisition and use of open source can potentially expose such business critical data.

The State of California Security Breach Information Act (SB-1386) regulates the privacy of personal information. The Act stipulates that if a security breach of a database containing personal data occurs, the responsible organization must notify each individual for whom it maintained information. Massachusetts has a similar law (Mass 201 CMR 17) that builds on SB-1386 with penalties up to $5,000 for each violation. Given the requirements for notification, the cost of violations and the fact that the US Federal Trade Commission estimates that as many as 9 million Americans have their identities stolen each year, development organizations need to ensure personal information is safeguarded.

EXPORT REGULATION

Governments around the world also regulate the commercial export and transfer of software containing encryption algorithms. To remain in compliance, organizations need to be aware of the cryptographic content of software and comply with applicable regulations. In the United States, rules governing exports and re-exports of software containing encryption items are administered by the Bureau of Industry and Security (BIS) or are found in the Export Administration Regulations (EAR), 15 C.F.R. Parts 730-774. There are over 4,000 open source projects with encryption algorithms strong enough to require a filing with the U.S. Department of Commerce Bureau of Industry and Security (BIS) if the code is exported from the U.S. Other governments around the world have similar regulations that control the type of encryption allowed to be exported and to whom.

SECURITY

Application security is an essential tool for managing risks in today's complex IT environment. According to Forrester, third-party code is not tested for quality, safety or security with the same level of rigor as in-house developed code. Security Week recently reported on data from a Forrester study of over 300 software development influencers in the U.S. and Europe that found 40 percent of respondents cited problems from third-

party code resulting in product delays or recalls, security vulnerabilities, increase in development time and revenue impact, which has caused these influencers to seek greater visibility into code integrity. Development's use of OSS can create blind spots that need to be addressed, and IT management needs to ensure security as new applications, products and services are created.

LEGAL

Legal risk and exposure with OSS is fairly well-known and widely reported. While open source is free, all open source comes with a license and obligations that must be met. Open source licenses range from simple/permissive licenses such as the MIT and BSD license, to the more restrictive, "copyleft" GPL family of licenses, including the AGPL that covers network access of open source over the Web. Improper use of open source code, especially code under the GPL-family of licenses, can impact an organization's IP and their brand. There have been a number of highly publicized lawsuits and violations with Fortune 500 companies that proved both embarrassing and damaging to the organizations' relationships with the open source community.

Understanding legal requirements for software has not been a developers job, but today's style of development increasingly relies on integrating external code, like open source, with the lack of formal acquisition processes. As such, governance needs to be put in place to both manage risk and empower developers to leverage open source for its significant advantages.

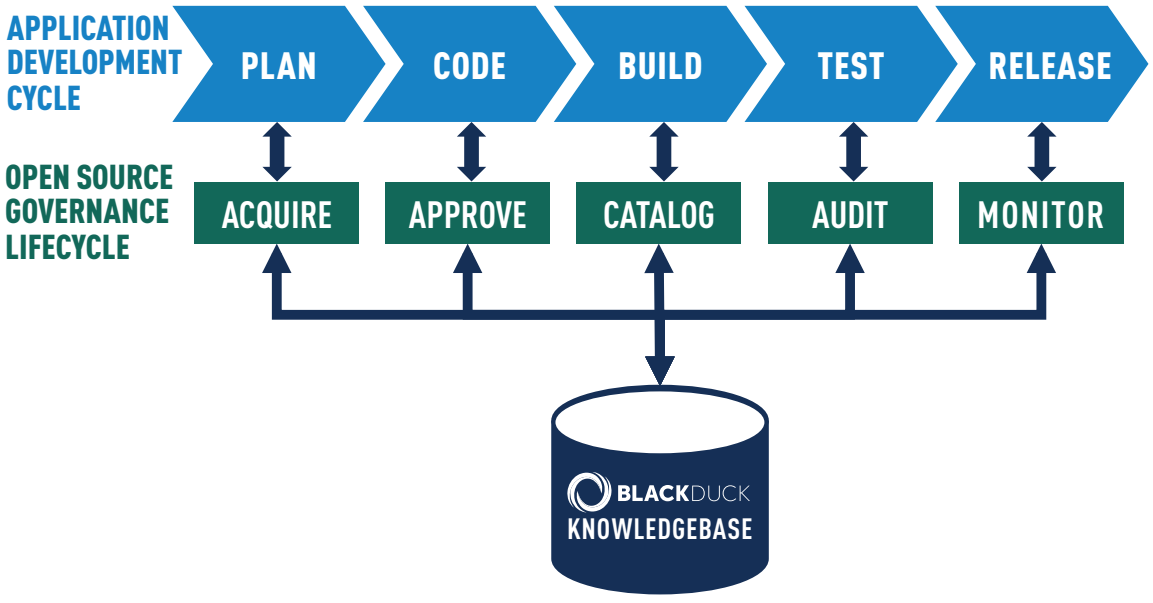
BRAND

A company's brand is one of its most valuable assets, representing the company's ultimate promise to all of its customers. A company's reputation reflects the management team's ability to deliver on the promise associated with its brand, and can affect:

- Stock valuation
- Access to capital/credit ratings
- Hiring, employee retention and engagement
- Relationship with open source community

While it can take years to develop a strong brand, it can take just one misstep to destroy it. The lawsuits in the open source world, for example, are highly visible examples of large enterprises – in many cases, Fortune 100 companies – being forced to comply with open source legal obligations, often at great cost to their brands and reputations. In addition, open source missteps impact an organization's relationship with the open source community, an increasingly strategic relationship for large development organizations.

Microsoft, for example, has made a concerted effort over the last few years to develop a positive relationship with the open source community. But even one of the best run software companies in the world ran afoul of the open source community and damaged its brand with the release of Windows 7. GPL licensed open source code was integrated with part of the release by a third-party and was not discovered as part of Microsoft's release process. To its credit, Microsoft discovered the problem, reported and fixed it. However, when



viewed in the context of Microsoft working to improve their relationship with the open source community, it was a significant setback to their development efforts and relationship with the community.

As Microsoft and others know, a company's relationship with the open source community is critical if they are to rely on what is, essentially, a volunteer community for help and support with code. In addition, this relationship is key to hiring open source talent; companies now strategically seek developers who are both skilled in software development and open source community savvy.

BLACK DUCK'S ROLE: ENABLING OPEN SOURCE GOVERNANCE

Effective governance of open source can empower developers, increase innovation and improve competitiveness. Black Duck enables organizations and developers to build better software faster by automating, managing and auditing their selection, use and governance of open source across the application lifecycle.

Black Duck customers realize the following results:

- IT controls to ensure developers use only approved, compliant third-party code
- Minimize risk and avoid painful business consequences
- Effectively monitor, audit and support applications that use open source
- Gain unprecedented visibility and control into all third-party code
- Increase developer productivity throughout the process
- Meet regulatory compliance goals

With nearly 1,000 customers around the world, Black Duck has the experience, scale and best practices to provide enterprise-scale governance that fully empowers developers with open source while virtually eliminating the operational, regulatory, security, legal and reputational risks.

ABOUT BLACK DUCK

Offering award-winning software and consulting, Black Duck is the partner of choice for open source software adoption, governance and management. Enterprises of every size depend on Black Duck to harness the power of open source technologies and methods. As part of the greater OSS community, Black Duck connects developers to comprehensive OSS resources through **Ohloh.net**, and to the latest commentary from industry experts through the **Open Source Delivers** blog. Black Duck also hosts the **Open Source Think Tank**, an international event where thought leaders collaborate on the future of open source. Black Duck is headquartered near Boston and has offices in San Mateo, St. Louis, London, Paris, Frankfurt, Hong Kong, Tokyo, Seoul and Beijing. For more information about how to leverage open source to deliver faster innovation, greater creativity and improved efficiency, visit **www.blackducksoftware.com** and follow us at @black_duck_sw.

To learn more, please contact:

UNITED KINGDOM & IRELAND
info-uk@blackducksoftware.com
or call +44 20 3290 0770

DACH
info-germany@blackducksoftware.com
or call +49 (69) 67733-196

FRANCE
info-france@blackducksoftware.com
or call +33 (0) 6 28 07 77 39

Additional information is available at: **www.blackducksoftware.com**

ABOUT BEARINGPOINT

BearingPoint consultants understand that the world of business changes constantly and that the resulting complexities demand intelligent and adaptive solutions. Our clients in commercial, financial and governmental segments enjoy real results when they work with us. We offer industry-based management skills, technological flair as well as functional expertise and the ability to adapt strategic insights to individual challenges. This adaptive approach is at the heart of our culture and has led to long-standing relationships with many of the world's leading companies and organizations.

BearingPoint has a proven track record of helping clients to strategically manage and exploit Free & Open Source Software (FOSS) driving cost reduction, innovation and productivity improvements while ensuring compliance with legal requirements. With our help clients have developed industry leading innovation models around FOSS sourcing and collaboration like the GENIVI Alliance of 150+ global automotive manufacturers and suppliers. We deliver FOSS services from strategy to implementation working with industry leading software vendors like Black Duck.

CONTACT

To learn more, please contact:

- Andreas Rindler at andreas.rindler@bearingpoint.com or +44 203 206 9670
- Claus-Peter Wiedemann at claus-peter.wiedemann@bearingpoint.com or +49 89 540336 367

Additional information is available at: **www.bearingpoint.com**