BLACKDUCK

BearingPoint®

OPEN SOURCE DRIVES INNOVATION IN FINANCIAL SERVICES

INTRODUCTION

The shift to mobile applications driven by consumers' expectations of ubiquitous services combined with the use of private cloud infrastructure is redefining the trajectory of IT investment and the competitive landscape for banks and financial service companies. Software development organizations at these institutions are faced with supporting, rationalizing and consolidating applications and platforms at a time when IT needs to increase innovation and agility, drive cost efficiency and accelerate software development.

The strategic use of open source software (OSS) can enable a financial services organization to use up to 60 to 80 percent open source software in their enterprise and mobility applications so they can do more and develop less. Yet according to Gartner, the average enterprise today uses only 29 percent open source code. When a financial services organization is able to put strategy, process and automation around finding, assessing, managing and scaling open source software reuse, it can revolutionize software development and increase innovation, flexibility and efficiency to gain a marketplace advantage.

THE CURRENT STATE OF TACTICAL USE

OSS is mostly used by financial services companies today ad-hoc by disparate application development organizations on a tactical basis, without standardized governance policies in place. While some financial services firms do use open source strategically by design, in most banks and insurance firms well-intentioned developers just search on the Internet for OSS that can be downloaded to add functionality to enterprise or customer-facing applications.

The use of OSS in financial services organizations today is often a tactical decision driven by innovative engineers seeking to solve problems. Any developer with a browser can search for code and download components, and in many cases this successfully achieves tactical objectives. But other versions of that same component may be used by another developer in the same department – or a functionally similar component may already be deployed – leading to the overhead of maintaining redundant code. OSS adoption is often engineering-driven, leaving the organization exposed to operational and technical risks and leaving the company with a tactically driven, ad-hoc process instead of a business strategy-driven adoption lifecycle that leverages technology to automate governance and achieve "built-in" compliance.

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, and engagement with the open source community can also lead to more efficient support models and increased developer productivity and retention. 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 prevent financial services organizations from maximizing the benefits of open source software while exposing them to risks.

REGULATORY COMPLIANCE

Regulatory compliance is concerned with meeting the obligations of regulations that may be affected by the use of open source. Open source is often an integral part of the applications that interact with critical business data. The lack of visibility into 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 intellectual property ownership.

With the macro-economic environment including tightening budgets and changes in governance driven by regulations such as Solvency II, MiFID and Basel II and III, the need to improve code quality, transparency and resource portability between projects has never been greater. For example, the Basel

II framework (and the forthcoming Basel III framework) specifies how much capital banks need to put aside to guard against the types of financial and operational risks that they face. 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 and 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 need for 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 companies can develop strategies and turn to automation tools and best practices to minimize and control regulatory risks. Banks and financial services companies need a strategic approach to the use of OSS that includes a clear definition of the business goals and drivers. And solid governance policies with an underlying automation technology platform to provide the evidence are needed for auditors to document regulatory compliance.

OPERATIONAL CHALLENGES

The technical and operational challenges resulting 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

Banks and financial services companies that take a tactical approach to the use of open source software need to implement strategic initiatives to protect against operational risks and against business continuity concerns arising from a lack of knowledge of the integrity of their software code. Easy Internet access and the ability to download, copy and paste code has circumvented formal software acquisition processes – a delight to many developers but a potential nightmare to development managers responsible for ensuring the integrity, quality and supportability of the software. Financial services organizations are faced with a lack of management, control and visibility into their code base. They are also dealing with managing technical support costs, since developers can download whatever open source components they find on the Internet and the organization can be left supporting multiple versions of components and multiple components that perform similar functions.

Outsourcing can create another set of challenges, since bringing in code from outside the organization or from outside the traditional supply chain can affect software integrity. It also raises regulatory compliance concerns; for example, Sarbanes Oxley requires corporate managers to validate the strength of internal controls, and MiFID places complex requirements on outsourcing important operational functions that materially impair the quality of internal control. While compliance personnel worry about the regulatory risks and the organization's ability to survive audits, IT personnel worry about the operational and support risks of open source code.

By taking a more calculated approach to the use of OSS, financial services organizations can gain unprecedented visibility and the ability to inspect and document all their source code. This becomes even more critical during merger and acquisition activities, as financial services organizations confront the need to scan the code of acquired organizations to understand and manage the risks inherent in depending on acquired software assets.

APPLICATION SECURITY

Application security, composed of a set of tools and practices, is essential for managing risks in today's complex IT environment, and the impact on code quality and service levels is an important consideration. According to Forrester, third-party code may not be tested for quality, safety or security with the same level of rigor as in-house developed code. Development's use of open source software can create blind spots that need to be addressed if IT management is to ensure security as new applications are created. Financial services institutions also have to ensure that data privacy is ensured to protect customer account information and ensure compliance with relevant regulations.

LEGAL EXPOSURE

Legal exposure with open source software must be clearly understood. While open source is free, all open source software has license obligations that must be met. Financial services organizations are increasingly investing in "mobile enterprise" infrastructure, creating more web-based applications that are accessible to customers on multiple platforms and which may trigger some of the reciprocity clauses of certain open source licenses. Open source licenses range from simple/permissive ones 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. And while many firms may track the most popular licenses, there are over 2,100 licenses with a variable set of obligations that financial services firms should track.

YOUR BRAND AND CUSTOMERS, SHAREHOLDERS AND DEVELOPERS

A financial services company's brand is one of its most valuable assets, representing the company's ultimate promise to all of its customers and shareholders. While it can take years to develop a strong brand, just one misstep can destroy it. Aside from lawsuits based on unmet open source license obligations however, it has become important for financial institutions to consider their brand perception among the developer community. A financial services company is only as good as its differentiated customer-facing financial applications, which depend more and more upon OSS and open source software developers.

With the overall maturation and adoption of open source increasing rapidly – and with many financial services companies like JP Morgan, Bank of America and NYSE Technologies designating open source use as strategic – a financial services organization's relationship with the developer community has become increasingly important. Many firms are "open sourcing" non-differentiated technologies and deeply embedding themselves in the open source community – in which the war for skilled resources is becoming fierce. Financial services firms cannot afford to make a misstep when using open source and engaging with the community, which may result in denigration of their "developer" brand.

COMPETITIVE ADVANTAGES FOR FINANCIAL SERVICES COMPANIES

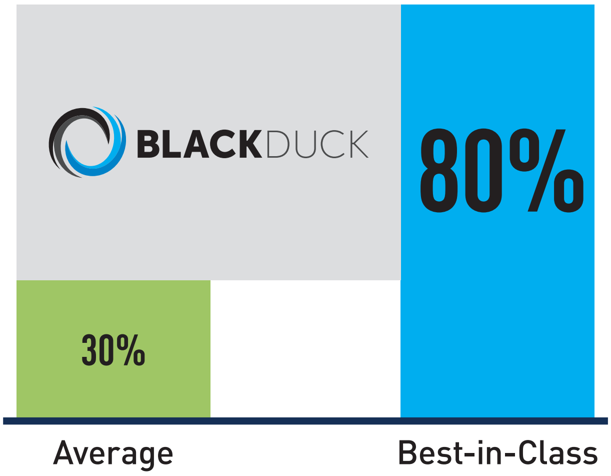
IT departments are under pressure to increase business flexibility and the velocity of innovation with the same or fewer resources. For example, as software development organizations within financial services organizations move from waterfall to agile development methodologies, they are faced with introducing new functionality within weeks and look toward the flexibility of open source software to address their business requirements. Using OSS, adopting agile development methods and standardizing internal code can help, but can also present management, control and compliance challenges that many banks and insurers have not yet addressed. Often, the extent of open source use in enterprise applications has not been documented and the implications are poorly understood.

Implementing a strategic software development approach that uses internal, external and open source components can:

- Complement the modular nature of agile methods
- Free developers to focus on real innovations
- Dramatically improve efficiency and mitigate expense pressure
- Increase developer productivity and retention
- Ensure visibility and control of software assets

As financial services firms race to deliver new applications and services using browser-based, mobile, cloud, content management and social media technologies, development resources are increasingly strained, creating IT backlogs.

The difference in open source use represents a large potential reduction of development



Open Source in the Code Base

investment that could be realized as cost savings, but more typically, financial services organizations shift that potential – with flat or declining development budgets – to areas that can create competitive value. Banks and insurance companies can leverage a strategic use of open source software to refocus resources on differentiation, and avoid reinventing the wheel by creating code that already exists.

THE IDEAL STATE FOR THE STRATEGIC USE OF OSS

In a study by Accenture, 73 percent of respondents said that open source was changing business IT, and according to Forrester, 79 percent of developers use open source. Gartner says that by 2014, 50 percent of Global 2000 organizations will experience technology, cost or security challenges through a lack of open software governance.

As financial services organizations move up the adoption lifecycle and evolve from being engineering-driven users to strategic adopters of open source software, they gain greater abilities to measure and manage progress in controlling the use of OSS according to defined policies. IT personnel become more active and more participative in open source communities, and as the adoption of OSS becomes driven by business strategy, banks and insurance companies can become leaders in the open source community and even take on sponsorship roles in creating standards and industry-driven communities.

As banks and insurance companies move up the OSS adoption lifecycle, the use of OSS becomes increasingly driven by business strategy rather than engineering necessity.

As open source becomes more commonly used throughout the organization, financial services companies need to develop a strategy to ensure that the proper controls and processes are in place to ensure compliance and reduce exposure. Financial services organizations need to develop open source governance strategies that focus on the specific issues related to the acquisition, use and management of OSS to ensure that this is done in alignment with the organization's stated objectives and policies.

For example, one large commercial bank recently developed a trading application that relied on 65 percent open source code. This bank was able to strategically leverage existing code already developed for other projects as well as third-party commercial code so that it only had to develop 28 percent of the unique code needed for this trading application. The net result was that use of open source governance, management and compliance tools allowed this commercial bank to deliver a new trading application while performing only 28 percent of the development work.

DEVELOP A DOCUMENTED OPEN SOURCE STRATEGY

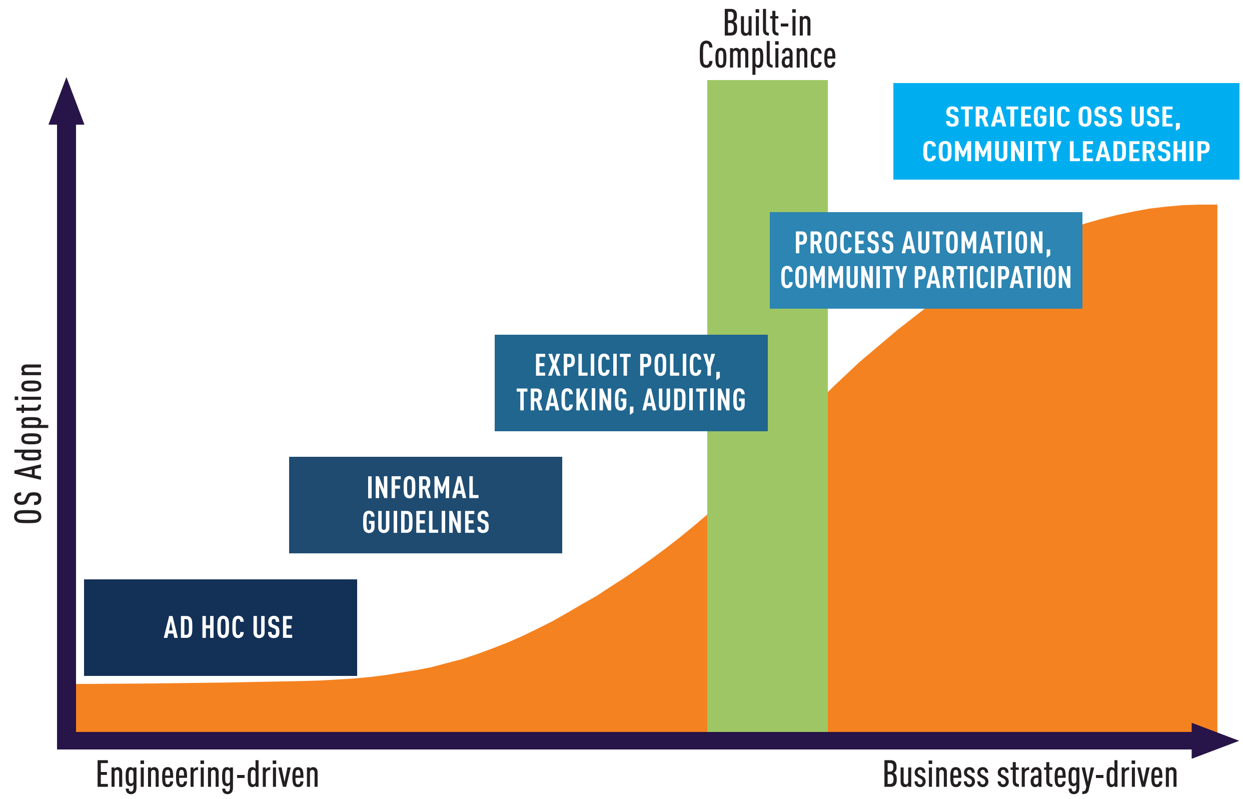
Financial services firms should begin by defining their strategy for OSS. The strategy should articulate the business objectives for using open source code. Most companies lack a documented strategy for using open source software, but having one is an important tool for establishing consensus and communicating the business rationale behind policies; without a defined strategy, an OSS adoption program is largely reactive. The strategy should address at a business level where open source will be used, what specific objectives will be accomplished and how they will be achieved.

ESTABLISH POLICIES AND PROCESS

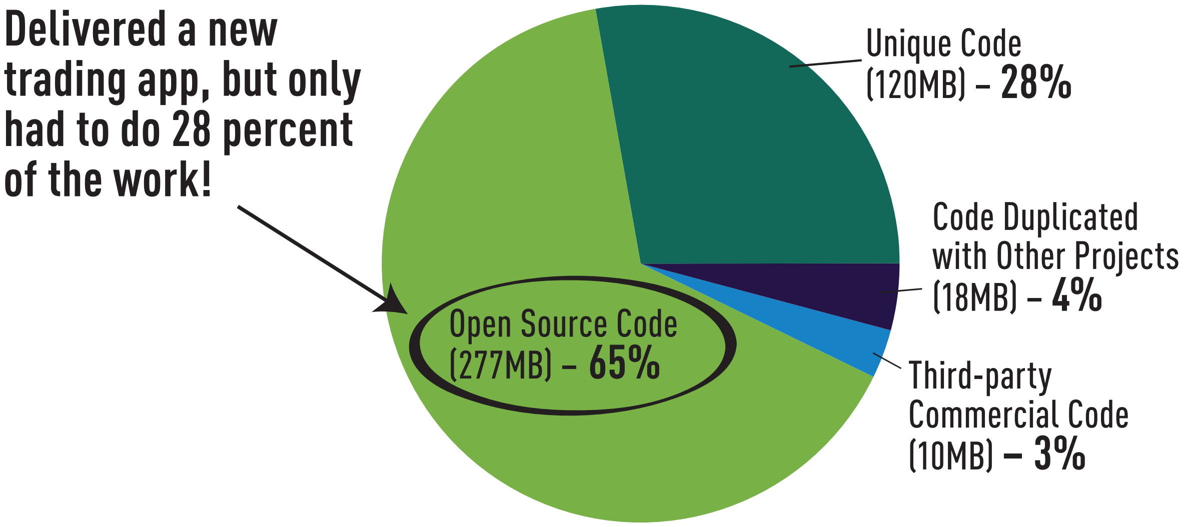
Financial services organizations need to establish policies that serve as the rules for evaluating, approving, using and releasing open source code, and for participating in communities. These policies should encourage developers to leverage the benefits of open source, and they should be created and managed by key stakeholders. Processes are also needed that define the way policies are reliably realized on a day-to-day basis. They need to be strategically interwoven with existing development and product release processes so that best practices can be maintained and the organization can streamline processes for component acquisition and approval, component updates, software releases and compliance.

LEVERAGE TECHNOLOGY

Manual processes for open source compliance are labor-intensive and error-prone; banks and insurance companies need to automate the key processes for effective management so they can design-in and automate policies to ensure ongoing compliance with relevant regulatory requirements and for ease of use so that developers will embrace the use of automation tools. Most financial services organizations employ software developers in multiple locations, and many leverage offshore developers. With the proper automation tools and processes for OSS management, strategic software development plans can be implemented and financial services organizations can successfully implement policies and processes while protecting against risks across an entire global software development environment.


Built-in Compliance
STRATEGIC OSS USE, COMMUNITY LEADERSHIP
PROCESS AUTOMATION, COMMUNITY PARTICIPATION
EXPLICIT POLICY, TRACKING, AUDITING
INFORMAL GUIDELINES
AD HOC USE
OS Adoption
Engineering-driven
Business strategy-driven

As banks and insurance companies move up the OSS adoption lifecycle, the use of open source software becomes increasingly driven by business strategy rather than engineering necessity



Delivered a new trading app, but only had to do 28 percent of the work!

The use of open source governance, management and compliance tools allows a large commercial bank to develop a trading application while only developing 28 percent of the code internally.

Financial services firms should implement the ability to search, select, analyze and audit open source code so they can consistently make better choices for acquiring code, and they need a configurable approval workflow that accelerates the approval process. Access to a catalog of approved components saves time and eliminates duplicate requests and redundant effort, and the ability to manage security vulnerabilities and cryptographic code ensures selection and use of the most secure open source components. The ability to index code is important because it increases developer productivity and ensures ongoing compliance.

Software development organizations increasingly use a complex multi-source development process that takes advantage of the abundance of open source components and building blocks available. Fully leveraging the use of open source requires tools built around a comprehensive knowledgebase and their integration into development workflows in order to automate key processes related to open source management throughout the application development lifecycle.

NURTURE INNOVATION

Open source platforms can be likened to working or playing with building blocks because developers are uninhibited by design constraints – they are free to innovate and develop new value and differentiation for enterprise applications. The flexibility and adaptability is unmatched by any proprietary platform. By developing a documented open source strategy, establishing policies and procedures and leveraging technology for effective open source management and governance, banks and insurance companies can accelerate software development, reduce costs and gain a competitive edge through the strategic use of open source software.

They can reduce risks and benefit from greater efficiencies, with standardization driving reduced version proliferation and reuse and control serving as an enabler for collaboration for software developers throughout the organization. Financial services companies can nurture innovation by focusing software developers on developing code that enables the achievement of business strategies – while relying on open source code wherever possible.

ABOUT BLACK DUCK FINANCIAL SERVICES SOLUTIONS

Black Duck Software enables banks and financial services companies worldwide to shorten time-to-solution and reduce development costs while mitigating the management, compliance and security challenges associated with open source software. Financial services firms can build better software faster by taking a strategic approach to open source software and automating, managing and auditing their selection, use and governance of open source across the application lifecycle. The Black Duck Suite is an advanced enterprise-class solution to the unique management, governance and security challenges associated with open source use by financial services organizations, and it automates key processes related to open source code management over the application development lifecycle.

Black Duck also offers a comprehensive range of professional services, including strategic planning services from its Olliance Group, to help financial services organizations develop strategies, policies and processes for managing open source, proprietary and third-party code, and prepare for the seamless integration of Black Duck's products into your organization. Our professional services team has more experience implementing open source software management solutions than any other company in the world. With over 1,000 customers around the world – including many financial services organizations – Black Duck has the experience, scale and best practices to help banks and insurance companies implement a strategic use of open source software that can accelerate software development, reduce costs and allow them to gain a competitive edge in the marketplace.

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**

BLACKDUCK

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

BearingPoint®

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**