




# The Corporate Counsel's Guide to Open Source Software Policy Implementation

*How to Protect the Enterprise from Risk while Helping Your Company More Efficiently Develop and Maintain Applications*

Black Duck Guidebook Series





Internal legal counselors increasingly face a common dilemma—how to enable enterprise software development teams to more efficiently leverage open source software (OSS) while protecting the enterprise from licensing risks. OSS is software for which the human-readable source code is made available under a copyright license. Software development teams can use, change and improve the software, and can redistribute it in modified or unmodified form. It is very often developed in a public, collaborative manner, and it is easily available to software developers via the Internet.

In the midst of a slowing economy, companies are faced with the challenges of reducing budgets while continuing to deliver innovative software applications that allow organizations to improve productivity and gain advantage in an increasingly competitive marketplace. This is why so many companies rely on open source software to complete software projects with fewer coding resources.

In fact when it comes to developers making use of open source, the genie is out of the bottle. Developers have been increasing their use of OSS even as corporate policies and management platforms lag behind. Adoption of OSS is becoming pervasive, and Gartner Group estimates that 85 percent of companies surveyed are currently using OSS. Software managers cannot be expected to be expert in licensing requirements, and attorneys cannot be expected to spend their valuable time reviewing source code and participating in the search, analysis and selection of OSS to support enterprise applications.

Lawyers can most efficiently allow the enterprise to benefit from OSS adoption by driving inter-departmental policies for evaluating the risks of implementing OSS and establishing guidelines and procedures that protect the enterprise while enabling development teams to more efficiently meet their business objectives. The legal staff is chartered with protecting the enterprise against risk—without creating policies that slow down the agility of the company. Successfully implementing OSS raises questions that internal legal counsel must be able to answer, such as:

- How can I avoid OSS license infringement lawsuits?
- How can I help development teams ensure licensing compliance—without creating a steady drain on the staff time of our legal team and on our budget for outside counsel?
- How can I be sure that the software we're developing does not include software components that violate licensing?
- How do we conduct due diligence for potential acquisitions to ensure the validity of software code that our company might acquire?
- How can we gather the information that lawyers, software developers and export personnel need to ensure compliance?
- How can I help our software development team take advantage of the economic efficiencies of OSS without them perceiving that their development progress is being slowed down by legal staff?

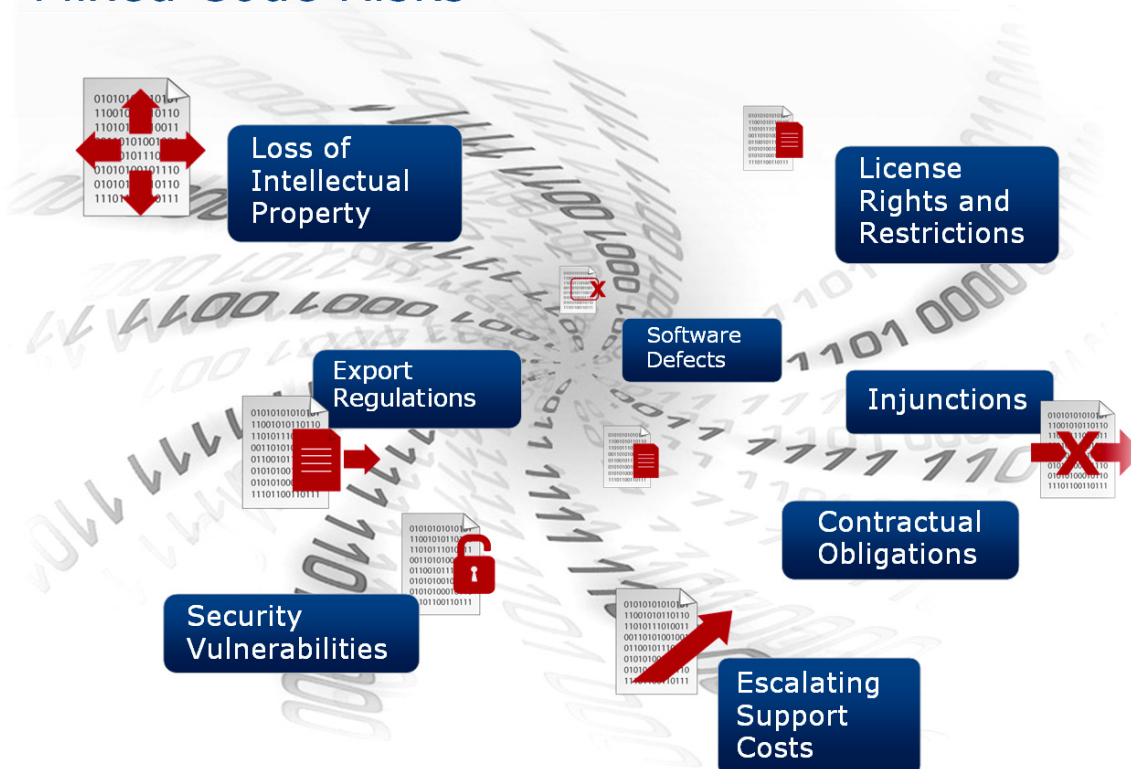
## Mitigating the Risks of Open Source Software


In this challenging economic climate, a company's ability to effectively find, integrate and manage open-source software is fast becoming as important as its own internal development capabilities. There are hundreds of thousands of open-source projects—and billions of lines of open-source software—readily available today for download, and most internal legal teams are understaffed for the demands of ensuring compliance with licensing requirements and protecting the enterprise against litigation risks.

The key to avoiding the consequences of improperly using the software is to develop policies and procedures based on best practices and automating the management of OSS code. Legal counsel needs to be able to understand the obligations associated with open source software licenses, and needs to foster the development of cross-departmental policies for protecting the organization from the business risks of violating software licenses. Companies can reap major rewards by leveraging OSS, but to do so effectively internal counsel must drive the development of policies and procedures to protect the enterprise and enable the safe and productive use of open-source software.

*Software development executives need automated tools to manage risk and reap the rewards of open source.*

## Mixed Code Risks





“Free code” does not mean “free of obligations”—open source brings with it unique and sometimes complex license and business risks that can delay, and potentially prevent, software deployment or shipment if not properly managed. A recent U. S. Federal appeals court decision in the Jacobsen versus Katzer case determined that Katzer had improperly used open source and was liable for copyright infringement as well as breach of contract. While this case set a new standard for open source license enforcement, it has also raised awareness with corporate counselors of the importance of explicitly managing what can be perceived as a free and unencumbered resource.

Compliance with applicable open source license obligations is key to avoiding the risk of costly and time-consuming litigation. Once a mere matter of proper attribution between developers and businesses, open source has now moved into the realm of the courts. In addition, the publicity surrounding today’s open source licensing issues can threaten the reputation and relationships of the defendant. Improperly managed open source code can result in bad publicity, copyright infringement and even stop shipment orders that damage company reputations and immediately impact product revenue streams.

There are notable examples of companies having to respond to charges that they did not adequately manage their use of open source code. Diebold was subject to a GPL infringement lawsuit over using Linux in its voting machines without complying with the GNU public license, and Google received bad publicity during the launch of its Android mobile platform because of known security law abilities. Skype was sued for violating

the GPL license for a VoIP phone, and Verizon was sued over the software license for open source software used in its wireless routers.

Understanding and managing open source license requirements is essential so the enterprise can avoid the risk of negative publicity and potential litigation. Manual methods of finding, selecting, monitoring and validating open source code are an unmanageable drain on law departments, and automation is essential so your company can efficiently incorporate OSS into its development efforts to drive down costs and efficiently manage applications throughout their lifecycles.

## Relying on Automation to Improve Productivity

Black Duck™ Software is the leading global provider of products and services for accelerating software development through the managed use of open source and third-party code. Black Duck enables companies to shorten time-to-market and reduce development and maintenance costs while mitigating the risks and challenges associated with open source reuse, including license obligations, security vulnerabilities and version proliferation.

While open source offers tremendous productivity enhancement opportunities, the ability to easily find and assess the best open source components is essential. The Black Duck KnowledgeBase—which tracks over 180,000 OSS projects—is the industry’s most comprehensive database of open source software and associated licenses and other information.

Engineers are paid to write, test, support and enhance code. They are not legal experts, and

you should therefore not expect them to serve as the internal authority on making business decisions on the use of open source code. The challenge is therefore to foster collaboration within the organization without locking down your development team in burdensome red tape. Many times, attorneys and developers have difficulty getting on the same page.

The dynamic nature of software development necessitates an automated framework that provides checks and balances and establishes rules of engagement for both lawyers and engineers. The successful use of open source requires the ability to treat the management of open source software as an integrated, cross-departmental business process, and not simply as a development process. Automation technology can streamline processes that are necessary for successfully managing the proper integration of code from many sources, and it can allow your software development teams to analyze the risks according to policies driven by legal counsel.

Attorneys can also leverage solutions from Black Duck to comply with export laws, such as the U.S. laws governing the export of software containing encryption. Black Duck offers the world's first and only solution specifically designed to facilitate encryption export compliance management for software and electronic devices containing software. Legal counsel worldwide depend on Black Duck solutions to analyze source code and identify cryptography within code in order to more quickly and easily comply with government licensing and documentation requirements for distributing software internationally.

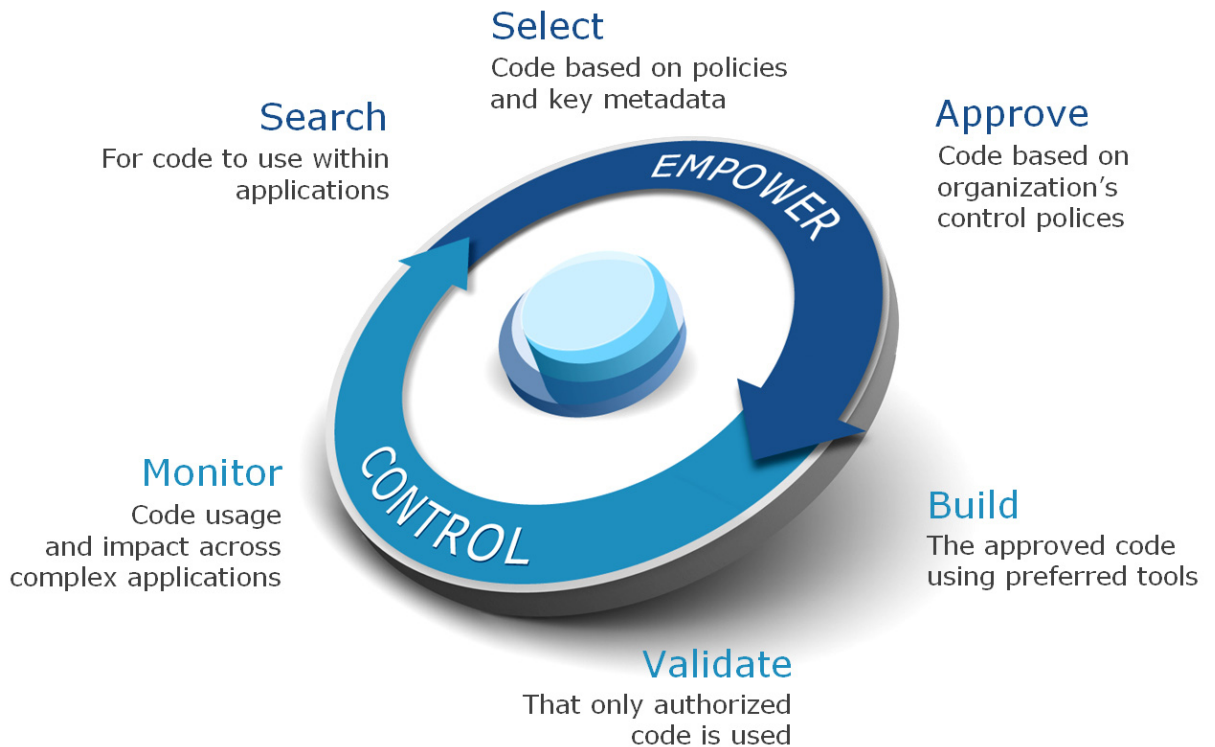
## Implementing Best Practices

Solutions from Black Duck Software allow attorneys to work closely with software development executives to implement best practices while streamlining development and making most efficient use of corporate resources. The following are just a few of the best practices that you will be able to develop policies for to protect the enterprise:

- Reuse existing components wherever appropriate
- Track and control changes to internal components
- Control reviews of sensitive or external components
- Verify every build and release
- Review compliance at project phase transition
- Create an audit trail of OSS usage
- Control component utilization
- Assess software components before making an acquisition

The enterprise can now rely on automated systems that liberate lawyers from conducting cumbersome legal reviews for the use of open source code. You can integrate your legal team with security, software development and other policy-making authorities within your company to streamline the use of OSS according to defined policies and procedures. This allows attorneys to increase transparency and enable development managers to safely utilize open source software.

*The enterprise can now deploy automated tools that can support the lifecycle of enterprise software applications.*



Having the knowledge to navigate through a maze of OSS components and their associated licenses can be extremely challenging, and manual methods place a tremendous drain on legal resources. But you can now simplify this otherwise daunting and time-consuming process by automating component search, selection and approval.

You can rely on proven tools to identify potential license conflicts, highlight discrepancies between business policies and intellectual property usage and provide an established framework for tracking issue resolution. You can now work closely with your colleagues in software development and security to establish enforceable policies for validating software contents, verifying license compliance and addressing any potential

issues early in the development cycle—before your company can allow itself to be exposed to business risks. Automation minimizes the manual efforts involved in designing, creating and maintaining software, and it allows legal counsel to protect the enterprise against licensing exposure while enabling more efficient and productive software development.

## Relying on Black Duck

It is impractical for any enterprise development organization to track and update the enormous pool of available open source code and its associated metadata. The Black Duck KnowledgeBase includes over 180,000 products from more than 4,000 sites and is updated with thousands of new products on a regular basis. Black Duck captures extensive metadata on

## Justifying M&A Activity

Voxeo Corporation makes voice applications easy to build and deploy, and as it sought to grow its business through the acquisition of an innovative Asian developer, management performed a rapid assessment of the value of the target company's software code base. According to Voxeo Vice President of Engineering Daniel Polfer, "We recognize that intellectual property laws vary throughout the world, and we wanted to fairly evaluate the code of the company we were acquiring to protect our investment and understand and document the value of the code." Manually evaluating the code was impractical, so Voxeo turned to the Black Duck Protex analysis system. A cross-departmental team consisting of legal counsel and engineering executives analyzed the code—and then proceeded through the acquisition with confidence.

"Before writing the check for the acquisition, we needed to identify what open source the company used and how they had used it," said Polfer. "Before we completed the deal, we were able to reduce our business risk by objectively assessing the software, understanding the licensing issues, and ensuring that we could safely leverage the code across our product line. We found that the selling company had fairly represented the integrity of their code. Protex allowed us to protect against any possible future issues with undocumented dependencies, and the assessment ultimately supported and helped justify the acquisition."

open source code, and the KnowledgeBase is continuously expanded. Black Duck has helped hundreds of companies automate the use of open source software, and some of the largest software companies in the world have standardized on Black Duck solution for implementing corporate policies without disrupting development efforts.

Black Duck provides a framework that allows attorneys to access timely and relevant information about OSS components used by the enterprise to effectively manage business risks. By automating the use of open source, you can effectively manage licensing compliance according to enterprise policies and procedures.

Black Duck Software is the leading provider of products and services for accelerating software development through the managed use of open-source and third-party code. Black Duck enables companies to shorten time-to-market and reduce development and maintenance costs while mitigating the risks and challenges associated with open source reuse, including hidden license obligations, security vulnerabilities, unsupported open source and version proliferation. By relying on solutions from Black Duck, legal counsel can avoid the potential pitfalls of mixed code development and help the enterprise efficiently develop and enforce an open source approval process for effectively managing business risks. To find out how your company can automate OSS implementations according to best practices, visit [www.blackducksoftware.com](http://www.blackducksoftware.com).

## To Learn More

We invite you to take advantage of a **free consultation** with one of our Open Source Software Specialists. Many have taken advantage of this free consultation to see how the Black Duck Suite can help protect your company from risk while helping your development organization more efficiently develop and maintain applications.

### *Please Visit*

[www.blackducksoftware.com/consultation](http://www.blackducksoftware.com/consultation) to schedule your free consultation. One of our OSS Specialists will be in touch to schedule your consultation on a day and time convenient to you.

If you wish to speak with someone right away, please call our customer hotline at 781-891-5100.

## About Black Duck Software

Black Duck Software is the leading global provider of products and services for accelerating software development through the managed use of open source and third-party code. Black Duck™ enables companies to shorten time-to-market and reduce development and maintenance costs while mitigating the risks and challenges associated with open source reuse, including hidden license obligations, security vulnerabilities and version proliferation. The company is headquartered near Boston and has offices in San Francisco, Amsterdam and Hong Kong, as well as distribution partners throughout the world. For more information, visit [www.blackducksoftware.com](http://www.blackducksoftware.com).



## Contact

To learn more, please contact:  
[sales@blackducksoftware.com](mailto:sales@blackducksoftware.com)  
or call +1 781.891.5100

Additional information is available at Black Duck's web site:  
[www.blackducksoftware.com](http://www.blackducksoftware.com)