PRACTICAL LAW COMPANY®

Open-source Software: Use and Compliance

Richard Raysman,
Holland & Knight LLP

This Practice Note is published by Practical Law Company on its PLCLaw Department web service at http://us.practicallaw.com/9-504-7111.

This Note discusses key issues and sets out practical tips for companies to consider to effectively govern its use of open-source software, both internally and when developing products.

Open-source software (OSS) is an important tool for helping businesses develop software rapidly and effectively, whether to run their internal systems or integrate into customer-facing products. While OSS can provide valuable benefits to a company, how a company uses OSS, together with the obligations contained in the software license granting the right to use that OSS, can have significant consequences. For example, it could:

- Affect the monetary value of company-owned intellectual property.
- Reduce a company's operational flexibility for developing and using certain types of software.
- Allow competitors to gain access to proprietary source code.
- Compromise a company's ability to execute on its long-term strategies.

To manage these risks, companies should have a plan in place to identify, implement and monitor the use of OSS, even if they are developing software solely for internal business purposes. Because the use of OSS spreads across several departments within a company, in-house counsel must be proactive in identifying these risks and developing a plan to implement and enforce appropriate policies and procedures.

This Note examines:

- How and why companies typically use OSS in their businesses (see *What is OSS?*).
- Common limitations and risks that arise when using OSS (see *How and Why Companies Use OSS*).
- Steps companies should consider in developing an OSS policy (see *Developing an OSS Compliance Policy*).
- Key provisions commonly included in OSS policies (see *Key OSS Policy Provisions*).

WHAT IS OSS?

OSS is computer software in source code form that is licensed to the general public at no charge under a copyright license that conforms to a set of standard criteria (known as the Open Source Definition). The criteria were developed by the Open Source Initiative (OSI) industry group, a nonprofit organization formed to promote and educate on the commercial use of OSS.

Source code is the form in which most software is originally written. It includes sets of alphanumeric instructions that contain words like "add," "move," "search" or "print." Source code is then passed through a software program (known as a compiler or interpreter) that translates the instructions into "object code." Object code is the form that a computer processes to execute a user's intended actions. It is numerically coded in sets of "0" or "1" (known as binary code). While people can read and understand source code, seldom can they understand object code. Therefore, to modify and maintain software efficiently, a software developer needs access to the source code. If there is an error in the code that needs to be fixed, a developer typically first updates the source code and then runs it through the compiler or interpreter to generate the updated object code.

Copyright © 2011 Practical Law Publishing Limited and Practical Law Company, Inc. All Rights Reserved.

Initially, much of OSS was developed by universities and nonprofit think tanks looking to provide a forum for the open development and improvement of software. The central rationale behind this movement is that freely licensed software is more useful for society because it could be improved more quickly and efficiently than proprietary software. For more information on the history and development of OSS, see *Practice Note, Open-source Software: OSS: The Historical Context (www.practicallaw.com/0-500-4366).*

There are tens of millions of lines of OSS source code available to developers at no charge. Some of the best known examples of OSS include:

- **Linux.** A computer operating system based on UNIX, the dominant proprietary operating system for personal and business computing in the 1970s and 1980s.
- **Mozilla Firefox.** A web browser first developed by Mozilla Foundation, a nonprofit organization dedicated to promoting openness, innovation and participation on the internet.
- **OpenOffice.** An application suite that includes components for creating and editing documents, spreadsheets, presentations, graphics and databases.
- **Apache HTTP Server.** A widely used web server software that has played an important role in the growth of the internet.

While OSS is usually available at no charge, it is not actually free. OSS is typically subject to a copyright license by the organization or individual who initially developed the software or is entrusted with enforcing the terms of the applicable license. Generally, OSS licenses permit licensees to use, copy, modify and redistribute the OSS, subject to complying with the disclosure, use, distribution and other relevant obligations and restrictions set out in the license. For more information on the limitations and risks in using OSS, see *Limitations and Risks in Using OSS.*

The OSI currently lists 67 different OSS licenses on its website. One of the best known OSS licenses is the GNU General Public License (GPL). For examples of key licensee rights and obligations under the GPL, see *Box, GPL: Key Rights and Obligations.*

HOW AND WHY COMPANIES USE OSS

Companies originally used OSS as stand-alone software primarily to support their internal operations. Today many companies:

- Combine OSS with their proprietary internal management or operations software.
- Include OSS in their customer-facing proprietary software.
- Integrate OSS into products, either as stand-alone software or with proprietary software, to be sold to customers.

For more information on how companies use OSS, see *Practice Note, Open-source Software: OSS: The Business Context (www.practicallaw.com/0-500-4366).*

OSS provides several commercial advantages for businesses. These include:

- **No license fees.** Businesses can avoid paying significant license fees by using OSS instead of similar proprietary software. For example, a business could use a Linux-based operating system instead of licensing the right to deploy a fee-based operating

GPL: KEY RIGHTS AND OBLIGATIONS

The GNU General Public License (GPL) is the most widely used OSS license. The GPL was implemented in connection with the GNU Project, which was formed in 1983 to encourage the collaborative development of free software, including a full operating system as a replacement to UNIX.

The GPL is the first "copyleft" license for general use, which means that derived works can only be distributed under the same license terms. The GPL provides, among other things, that:

- The licensee:
  - may copy and distribute the OSS source code to any third party;
  - must conspicuously publish a copyright notice and disclaimer of warranty;
  - may charge a fee for the physical act of transferring a copy to a third party; and
  - may modify and distribute the OSS source code, provided that the modified files carry prominent notices that they have been changed, any modified program that in whole or in part contains the original OSS must be licensed at no charge to all third parties and the licensee displays a notice that there is no warranty for the modified OSS.
- The requirements under the GPL apply to the modified work as a whole. However, if identifiable sections of the code are not derived from the OSS and can be reasonably considered independent and separate works themselves, then the OSS license terms will not apply to those sections distributed as separate works.
- The licensee may distribute the OSS object code separately, but it must be accompanied by an offer to provide the OSS source code at no charge.
- If the modified OSS code is distributed in violation of the license, then the original OSS license is void and automatically terminated.
- The recipient of the modified software cannot have any further restrictions on the right to modify or distribute that software.
- There is no warranty and the OSS is provided "as is."
- In no event will the party who modifies and distributes the OSS be liable for damages.

Copyright © 2011 Practical Law Publishing Limited and Practical Law Company, Inc. All Rights Reserved.

system. From a cost-basis standpoint, OSS is especially valuable for small businesses and start-ups looking to use effective software on a tight budget.

- **Reduced development time and expense.** Software developers are often under pressure to meet deadlines and expense budgets. For a developer, it may be more efficient to download and integrate existing OSS code instead of writing new code.
- **Use of reliable code.** Instead of developing untested software, software developers can use OSS source code that has been openly tested, used and improved by others.
- **Ability to maintain and improve the code.** To have workable software that a software developer can modify and maintain, the developer must have access to the source code. However, most proprietary software is licensed solely in object code format, making it impossible for the licensee to actively maintain or improve the software. If the software's functionality declines and requires maintenance, the licensee must go back to the software owner or a third party authorized by the licensor to perform maintenance. In contrast, an OSS user can modify the code on its own.
- **Access to third-party improvements.** Some OSS licenses require licensees to disclose any modifications or improvements they make to the OSS code to the licensing organization. This disclosure requirement allows other licensees to access and implement improvements that they may be unable to develop themselves.

LIMITATIONS AND RISKS IN USING OSS

There are several barriers to successfully integrating OSS into a company's information technology (IT) systems. Although OSS licenses vary widely in scope, application and legal effect, most include certain underlying obligations and restrictions. Along with these limitations are various risks associated with OSS use that can threaten a company's valuable intellectual property rights. In addition, a growing number of copyright owners have recently been pursuing the enforcement of OSS licenses through litigation.

LIMITATIONS

OSS licenses can contain many obligations and restrictions on how licensees may use, modify, integrate or distribute OSS. An OSS license may provide, for example, that if the licensee distributes software containing OSS code to third parties, it must:

- Do so under the same OSS license from which that code was initially licensed.
- Place no restrictions on the recipient's right to modify or distribute the OSS beyond what is provided in the applicable OSS license.
- Make that product's corresponding source code available to the recipient.

An OSS license may also include a requirement for the licensee to contribute any modifications, improvements or other derivative works the licensee develops back to the original OSS code base for others to use or develop. For more information on OSS licenses and corresponding obligations and restrictions that may apply, see *Practice Note, Open-source Software: The OSS Licenses (www.practicallaw.com/0-500-4366).*

RISKS

Companies that use OSS, whether intentionally or inadvertently, without an OSS use and compliance plan face certain legal and business risks, such as:

- **Risk to intellectual property.** Incorporating OSS into a company's software can affect the proprietary nature of its intellectual property. Depending on the terms of the license under which a company is using certain OSS, it may inadvertently cause intellectual property rights in its proprietary software, including any confidential algorithms and related trade secrets, to enter the public domain if it fails to integrate the OSS properly. This can affect the value of the software and, to an extent, the company itself.
- **Risk to future revenue.** Some companies develop software internally that they might want to commercialize or sell at a later date, either as a stand-alone product or as part of the company's acquisition. The integration of OSS into a company's software could dilute the commercial value of the product and compromise the company's ability to fully exploit its commercial potential.
- **Acquisition risk.** Without performing adequate due diligence, companies risk acquiring software, or a company whose assets include proprietary software, that has a diluted value because of the inclusion of OSS.
- **Competitive risk.** Depending on the terms of the relevant OSS license, incorporating OSS into a company's proprietary software and redistributing it to employees, suppliers, contractors or customers could result in that software being considered part of the public domain. This would allow the company's competitors to access its code at no charge.

RISING LITIGATION

Historically, few cases have been brought against licensees for their use of OSS. Recently, however, copyright owners have been more aggressively enforcing the terms of OSS licenses against alleged infringers, claiming that violations of an OSS license create liability for copyright infringement.

Jacobsen v. Katzer & Kamind Associates, Inc.

In an opinion viewed as a major development in open source law, the US Court of Appeals for the Federal Circuit ruled that failure to comply with the conditions of an OSS license may constitute copyright infringement. In *Jacobsen v. Katzer & Kamind Associates, Inc.*, the Federal Circuit held that the terms of an OSS license governing users' modification and distribution rights were limits to the scope of the license, and a failure to comply with those terms could form a viable copyright infringement claim. The court stated that compliance with open source requirements, while different than traditional licensing fees in the commercial setting, were entitled to no less legal recognition (*Jacobsen v. Katzer & Kamind Assocs., Inc., 535 F.3d 1373 (Fed. Cir. 2008)*).

Copyright © 2011 Practical Law Publishing Limited and Practical Law Company, Inc. All Rights Reserved.

Software Freedom Conservancy Inc. v. Best Buy Co., Inc. et al.

Another copyright infringement case that is considered significant for OSS licensors and the OSS community as a whole is the ongoing matter of *Software Freedom Conservancy Inc. v. Best Buy Co., Inc. et al.* Software Freedom Conservancy (SFC) is alleging that various electronics retailers and manufacturers sold and distributed electronic products, such as high-definition televisions, digital video recorders, DVD players, video cameras and wireless routers, embedded with firmware that contained a copy or a derivative work of OSS known as BusyBox without complying with the terms of the GNU General Public License, version 2 (GPLv2) (*Software Freedom Conservancy Inc. v. Best Buy Co., Inc. et al., No. 09-10155 (S.D.N.Y. filed Dec. 14, 2009)*). Although still pending, this case highlights the importance of complying with the licensing terms of OSS. For more information on the enforcement of GPLv2, see *Practice Note, Open-source Software: Current OSS Legal Issues (www.practicallaw.com/0-500-4366).*

Free Software Foundation, Inc. v. Cisco Systems, Inc.

OSS licensors have also recently taken action to compel companies that use OSS to comply with the obligations set out in the applicable OSS license. In a case involving the Free Software Foundation, Inc. (FSF) and Cisco Systems, Inc., FSF brought an action against Cisco to force it to publish source code that Cisco acquired with its acquisition of The Linksys Group Inc. Linksys had incorporated another company's software containing OSS into its own proprietary software, and the license to which the OSS was subject required OSS users to provide public access to the complete and corresponding source code of its underlying software (*Free Software Found., Inc. v. Cisco Sys., Inc., No. 08-10764 (S.D.N.Y. filed Dec. 11, 2008)*).

For more information on these cases, see *Box, Rising Litigation.*

DEVELOPING AN OSS COMPLIANCE POLICY

OSS policies can be structured in many different ways depending on how a company intends to use OSS in consideration of its overall business objectives. Some types of policies are designed solely to manage a company's use of OSS in its internal business, while others are structured to also accommodate the incorporation of OSS in customer-facing products. A company should carefully consider how best to design the OSS policy to meet its risk management objectives without compromising operational flexibility or overly burdening personnel.

Once a company has committed to implementing an OSS use and compliance program, it should take the following steps to develop the governing OSS policy:

- **Understand the company's business objectives.** Counsel should first communicate with the key business stakeholders to develop a common understanding of how the company uses or intends to use OSS, and determine how the intended use of OSS best aligns with company's overall business, intellectual property and risk management goals.
- **Evaluate current OSS procedures, if any.** Counsel should coordinate with personnel responsible for managing software development, use and maintenance (typically the chief information officer or equivalent) to identify and review any current OSS risk management processes. Together, counsel and the relevant personnel should identify any gaps in these processes, and note the corresponding business and legal risks that may result from these gaps. This step should be carried out in a collaborative manner to encourage interdepartmental agreement and minimize the risk of being considered intrusive.
- **Understand how software is or will be developed.** With the exception of companies in the software business, most software development work is outsourced to third-party developers. However, third-party developers sometimes attempt to accelerate the development process and save time by using existing OSS without the customer ever knowing. Additionally, many third-party developers subcontract work to software engineers residing overseas. As a result, counsel may need to navigate through several layers to find out where the development is ultimately taking place to effectively identify and address OSS use by third-party developers.
- **Set up an OSS working group.** Companies should form a working group of key stakeholders (including legal, IT, operations and management) to evaluate relevant business goals, and develop an OSS strategy and policy. The roles, responsibilities and leadership of group members should be clearly communicated.
- **Appoint an OSS compliance officer.** An individual should be designated to act as the chief compliance officer to:
  - drive development and implementation of the OSS policy;
  - monitor OSS use and ensure that employees and third-party contractors are complying with the OSS policy;
  - train personnel on the OSS policy and the appropriate use of OSS; and
  - regularly advise the OSS working group on issues or risks that may arise.

Because the risks of using OSS are so significant, companies typically appoint a senior manager who is already employed in the company's IT or compliance department.

- **Develop an OSS use strategy statement.** A company can provide operational direction for its business units on developing and adopting an OSS policy by creating a short, concise strategy statement that sets out the company's high-level business objectives for using or acquiring OSS. By clearly communicating its objectives, a company's business units can more easily coordinate on implementing an OSS policy that helps, rather than obstructs, the overall operation of the business. When drafting a strategy statement, a company should ensure that its approach to using, or not using, OSS should be tailored to complement its overall product development, revenue generation and cost containment plans.
- **Develop a plan for creating and implementing the OSS policy.** Once the company has finalized its OSS strategy,

Copyright © 2011 Practical Law Publishing Limited and Practical Law Company, Inc. All Rights Reserved.

RISING LITIGATION

JACOBSEN V. KATZER & KAMIND ASSOCIATES, INC.

In *Jacobsen*, the court considered a copyright holder's ability to dedicate certain work to free public use and yet enforce an open source copyright license to control the future distribution and modification of that work (a nonexclusive OSS license).

The plaintiff owned a copyright to a computer programming code and made it available for public download under an OSS license. The license required parties distributing software that incorporates the plaintiff's copyrighted OSS to:

- Display attribution to the original copyright owner.
- Note changes to the original code so that downstream users could follow improvements.
- Place the user's modifications in the public domain.

The defendants allegedly incorporated certain aspects of the plaintiff's software into one of the defendant's commercial software packages without following the terms of the license.

The district court determined that the defendant's alleged violation of the conditions of the license may have constituted a breach of the nonexclusive license, but it did not create liability for copyright infringement (*Jacobsen v. Katzer, No. 06-CV-01905 JSW, 2007 WL 2358628 (N.D. Cal. Aug. 17, 2007)*).

On appeal, the Federal Circuit vacated and remanded the district court's decision and held that the terms of the license governing users' modification and distribution rights were limits to the scope of the license and could form a viable copyright infringement claim. The court stated that compliance with open source requirements, while different than traditional licensing fees in the commercial setting, were entitled to no less legal recognition (*Jacobsen v. Katzer, 535 F.3d 1373 (Fed. Cir. 2008)*).

On remand, the US District Court for the Northern District of California denied the plaintiff's motion for a preliminary injunction because of a lack of showing of irreparable potential harm stemming from the defendant's alleged copyright infringement (*Jacobsen v. Katzer, No. C 06-01905, 2009 WL 29881 (N.D. Cal. Jan. 5, 2009)*). However, the district court subsequently granted the plaintiff's motion for summary judgment on the copyright claim on liability only and granted in part the plaintiff's motion for summary judgment on its Digital Millennium Copyright Act claim for the defendants' removal of copyright management information from the plaintiff's software code (*Jacobsen v. Katzer, No. C 06-01905, 2009 WL 4823021 (N.D. Cal. Dec. 10, 2009)*).

Following these rulings, the parties settled the matter. The defendant agreed to a permanent injunction that bars it from improperly using the plaintiff's software and further agreed to pay a judgment of $100,000 in the plaintiff's favor (*Jacobsen v. Katzer, No. 06-01905 (N.D. Cal. Feb. 18, 2010)*).

FREE SOFTWARE FOUNDATION, INC. V. CISCO SYSTEMS, INC.

In *Free Software Foundation*, the FSF sought to require Cisco to publish source code that it acquired when it purchased Linksys. The FSF alleged that Cisco, through its acquisition of Linksys, distributed products containing infringing firmware that incorporated the plaintiff's open source programs without complying with the terms of the GPLv2. The FSF asserted copyright infringement claims for the defendant's alleged violation of the conditions of the open source license.

According to the FSF's complaint, Linksys' products containing GPL-licensed source code had been part of a supply chain, where Linksys acquired certain internal computer chips from a supplier who had previously outsourced the development of the chips to an overseas entity that apparently had employed the GPL-licensed code. After the acquisition, Cisco allegedly distributed the relevant software and refused to publish the source code. The FSF brought copyright infringement claims alleging that Cisco violated the GPLv2 by refusing to make the source code publicly available. For more information on GPLv2's licensing obligations, see *Practice Note, Open-source Software: Current OSS Legal Issues (www.practicallaw.com/0-500-4366).*

The parties eventually settled the matter without Cisco having to release the source code, but Cisco agreed to:

- Appoint a free software director for Linksys who must make ongoing compliance reports to the FSF.
- Notify Linksys customers of their rights under the GPLv2.
- Publish compliance license notices.
- Make complete, corresponding and up-to-date source code available on its website.
- Make a monetary contribution to the FSF.

SOFTWARE FREEDOM CONSERVANCY INC. V. BEST BUY CO.

In *Software Freedom Conservancy Inc.*, an open source developer and the Software Freedom Conservancy filed a copyright infringement suit against various electronics retailers and manufacturers for allegedly selling and distributing electronic products embedded with firmware that contained a copy or a derivative work of the plaintiff's OSS without complying with the terms of GPLv2,

Copyright © 2011 Practical Law Publishing Limited and Practical Law Company, Inc. All Rights Reserved.

RISING LITIGATION (CONTINUED)

the license under which the OSS is made publicly available. Specifically, the plaintiffs are alleging that each defendant failed to provide either the complete corresponding source code for the OSS or a written offer to provide the source code when the defendants distributed the electronic products.

Although the matter is still pending, on July 27, 2010, the US District Court for the Southern District of New York granted the plaintiffs' motion for default judgment against one of the defendants who was insolvent and refused to participate in the litigation. The court held that the defaulting defendant was liable for willful copyright infringement and granted the plaintiffs' request for a permanent injunction as well as statutory damages and attorney's fees. While the court's decision to recognize copyright infringement for allegedly violating the GPLv2 is significant for the plaintiffs and the OSS community as whole, the claims against the remaining defendants are still pending.

the OSS compliance officer, in consultation with the OSS working group, should develop the OSS policy and a plan for implementing it. The plan should address:

  - training personnel on following applicable provisions of the policy;
  - communicating with third-party contractors on the policy and compliance expectations;
  - developing measures to identify OSS and monitor its use;
  - updating commercial contracts to incorporate required OSS-related provisions; and
  - taking post-implementation steps to evaluate and update the policy as needed.

- **Ensure that the OSS policy represents an actionable plan.** Beyond identifying the company's objectives concerning the use of OSS, the OSS policy should:
  - be concise and clearly worded to avoid ambiguity and ensure that employees and third-party contractors are aware of their respective responsibilities;
  - identify applicable roles and responsibilities for employees and third-party contractors who may be involved in the development or deployment of software that contains OSS;
  - set out the criteria and decision points for OSS use;
  - identify information to be collected and tracked; and
  - include the name and contact information of the OSS compliance officer and any other key employees responsible for implementing the policy and enforcing its guidelines.

KEY OSS POLICY PROVISIONS

OSS policies, in their various forms, typically address the following key issues:

- Management and administration of OSS use (see *Management and Administration).*
- Guidelines for software development and OSS integration (see *Development and Operational Guidelines).*
- OSS risk prevention (see *Additional OSS Risk Prevention Provisions).*

MANAGEMENT AND ADMINISTRATION

An OSS policy must identify the relevant personnel responsible for managing OSS use within the company and specify what employees are covered by the policy. This section usually deals with:

- **Roles and responsibilities.** Identifies who should receive OSS-related questions and information requests. Also lists departments and personnel responsible for action items under the policy (for example, the point of contact for administering OSS source code disclosure requests).
- **Employee access.** Requires distribution of the policy to key employees and their training, as applicable, on the systems and processes necessary for using OSS. Some companies require a receipt of training acknowledgment from employees to deliver to any outside auditors that may request verification.
- **Contract language.** Sets out the appropriate legal language to be inserted in applicable customer contracts for the sale of products or services that use OSS or, alternatively, the procedure for requesting the legal language. If the company maintains form OSS-ready contracts, the policy should state how the appropriate business parties can access them.
- **Third-party compliance.** Lists steps that the relevant employees should take to ensure that all third-party contractors are aware of the guidelines for OSS use and understand their responsibilities under them.

DEVELOPMENT AND OPERATIONAL GUIDELINES

At the center of an OSS policy are the steps employees must follow to use and develop OSS. These provisions set out guidelines regarding:

- **Integration approvals.** Sets out clear guidelines on when OSS can be integrated with proprietary software and who may authorize it. This reduces the risk of OSS infecting the company's proprietary software.
- **Integration requirements.** Describes how OSS can be integrated with the company's proprietary software. Typically, companies require their developers to ensure that the OSS is sufficiently segregated from their proprietary software, often by creating interfaces between an OSS module and a company's proprietary software that allow each to operate as independent modules.
- **OSS license information.** Specifies that the license agreement associated with the OSS must be printed out and retained. The OSS

Copyright © 2011 Practical Law Publishing Limited and Practical Law Company, Inc. All Rights Reserved.

compliance officer should maintain copies of all these licenses and coordinate with the OSS working group to ensure that the company complies with the terms of each license. The officer should also have copies of most or all of the other existing OSS licenses that are publicly available to reference against the applicable license.

- **Development controls and checkpoints.** Sets out the relevant controls and checkpoints to be implemented during the "build" phase of a software development project, including:
  - when OSS is first added to a software build;
  - when internally developed software is created or modified;
  - at each transitional phase in the software development process; and
  - when considering modifications on an OSS project.
- **Component review periods.** Identifies at what phase or phases of development the component review process should take place.
- **Verification phase.** Creates a defined verification phase when questions can be posed about all components of a software product before its final release.
- **Documenting modifications.** Requires any modifications made to the OSS to be documented. This can be done by flagging all of the original OSS code with a code identifier and requiring software developers to include code identifiers in any further modifications to the code.
- **Headers.** Provides that headers in the OSS code should not be altered and developers should retain any comments previously included in the code headers.
- **Re-naming.** Instructs that, to the extent possible, developers should not re-name modules in the OSS code. Maintaining the original module names will make it easier later on to trace the original OSS source code.
- **Interface documentation.** Requires developers to carefully document all software interfaces that are created to allow a company's proprietary code to interact with OSS.
- **Scanning.** Determines when to scan for OSS code. Some companies scan for all OSS code during development. This can be time consuming, but it is a good way to preserve a snapshot of what OSS is being used at each phase of the project and subsequently track its integration.

ADDITIONAL OSS RISK PREVENTION PROVISIONS

To minimize the risks associated with OSS use, an OSS policy generally requires careful due diligence before obtaining or incorporating the OSS. This includes:

- **OSS audits.** Calls for an audit of the software code to determine the existence of any OSS whenever a company is considering acquiring or licensing business-critical software. Companies often turn to third-party specialists to conduct this type of due diligence.
- **Intellectual property due diligence.** Requires an evaluation of the potential risk to any intellectual property strategies before the integration of OSS with proprietary software is allowed. Even small changes to OSS code can affect a company's ability to file for patents or may affect an existing patent license.
- **OSS license due diligence.** Requires a check to determine if there is a better alternative to OSS software that is subject to an overly restrictive license. Before turning away from using the OSS, a company should first check whether different software that is similarly functional can be obtained under a different, less restrictive license.
- **Monitoring OSS use and enforcing the OSS policy.** Provides guidelines for tracking the use of OSS and ensuring that a company's employees and third-party contractors are complying with the OSS policy. For example, a company can implement a reporting system (whether written or online) to track when employees or contractors integrate OSS during each phase of project development. This type of system would allow companies to monitor OSS use from the very beginning of the project and inform senior management of the company's use of OSS early in the process.

Practical Law Company provides practical legal know-how for law firms, law departments and law schools. Our online corporate, securities and finance resources help lawyers practice efficiently, get up to speed quickly and spend more time on the work that matters most. This Practice Note is just one example of the many resources Practical Law Company offers. Discover for yourself what the world's leading law firms and law departments use to enhance their practices.

Contact Us

Practical Law Company
747 Third Avenue, 36th Floor
New York, NY 10017
646.562.3405
plcinfo@practicallaw.com
www.practicallaw.com

Copyright © 2011 Practical Law Publishing Limited and Practical Law Company, Inc. All Rights Reserved.
Use of PLC websites and services is subject to the Terms of Use (http://us.practicallaw.com/2-383-6690)
and Privacy Policy (http://us.practicallaw.com/8-383-6692).