

Hot Issues

Auditing compliance with software license agreements

April 22, 2002

Dixie Walters
KnowledgeSpace contributing writer

Compliance with software licensing agreements may not be one of those topics that companies are overly concerned about. But in the current economic environment, perhaps they should be. Software vendors, squeezed for new revenues, have stepped up their audits to ensure that companies are not using unlicensed software.

"In tight economic times, software vendors will look at every avenue that might help them to generate revenue, and ensuring customers pay for all copies of their software provides one such route," according to Gartner analyst Patricia Adams. Furthermore, the environment is ripe for software vendors to receive tips about software piracy. After all, the best source of piracy tips is former employees, and those ranks have swelled in the wake of widespread layoffs.

"If a company has unhappy ex-employees and the company's been dealing in unlicensed software, I'd say there's a pretty good chance (of being audited) because that's usually where they get most of their leads," says Jim Brey, a senior manager in Andersen's technology risk consulting practice in Portland, Oregon. Brey notes that in the Pacific Northwest region, the Business Software Alliance (BSA) advertises frequently, seeking tipoffs on illegal software use.

Illegal use of software occurs in many ways. According to Gartner research, some common problems are: users downloading software and then using it on corporate computers without authorization, the sharing of user names and passwords for software or software services, complex changes to vendor licensing terms and conditions that result in confusion and misuse, and inadvertent violations stemming from mergers, acquisitions or divestitures.

The software industry takes piracy in any form very seriously. The BSA estimates that software piracy costs the global economy more than US\$14 billion a year in lost revenue. Companies caught using unlicensed or illegal software face severe consequences.

In addition to significant fines -- civil penalties of up to \$150,000 for each program copied and criminal penalties of up to \$250,000 and possible imprisonment -- there are other risks. Illegal software comes without documentation, warranties or technical support. It also may carry destructive viruses and comes without benefits such as upgrades and fixes. If a company is caught using software illegally, it faces potential damage to its reputation as well. The BSA and the Software and Information Industry Association, another trade group, make a point of publicizing the results of their enforcement efforts with news releases.

With so many potential risks, internal auditors want to do all they can to help their companies minimize the risks of noncompliance with software license agreements. Here are some things auditors can look for:

Ensure that the company has an anti-piracy policy. Companies should have a policy indicating that they support computer software copyrights and expect users to adhere to license agreements. The Software &

Information Industry Association (SIIA) has a [sample](#) of corporate user policies and procedures that can be customized to individual companies. The BSA offers similar [documents](#).

The trade groups suggest that companies distribute software usage policies in new employee packets and that all employees acknowledge the policy through some type of acceptance feature. Gartner suggests that the compliance policy also include a component that holds employees liable for illegal software usage. As part of a concurrent educational effort, employees need to be informed about what entails illegal usage, including actions such as bringing software from home and loading it on the company's computer or vice versa, when this violates the license agreement.

Brey notes that, whenever possible, companies should have information security controls in place that prevent individual users from loading software on the company's computers in the first place. As for anti-piracy policies, Brey says, "If a company doesn't have these policies, then red flags should come up because people are going to do whatever they think they need to do to get their jobs done -- and sometimes people think they need to bring in a piece of software from home."

Verify that all software purchases go through a centralized purchasing process. To keep tabs on the software being acquired and, therefore, ensure compliance with licenses, companies will want to require that all software purchases be approved through centralized purchasing, rather than allowing employees to make individual software purchases and seek reimbursement through their expense accounts. With centralized purchasing, companies can verify that software purchases are made from reputable parties and that the software comes with the proper documentation and license agreements.

Maintain an accurate inventory of software assets. Before you can monitor compliance with license agreements, "you need an inventory of your software so that when you do a periodic audit, you know what you're comparing against," Brey says. Numerous auditing software tools are available to help companies get a picture of the legal and illegal software that's installed on their computers. Through an inventory, companies can identify illegal software that should be deleted, as well as determine whether unused or outdated software exists that could be deleted. As part of the inventory, the BSA advises companies to collect the product name, version number and serial number for every copy of software installed on the company's network. Software should then be matched with licenses, manuals, receipts and other important documentation. In particular, auditors will want to establish the number of copies or users allowed by the various license agreements.

Brey says software inventories are useful in finding accidental instances of illegal use. This often occurs when companies redeploy computers to other parts of the company. For instance, he says a computer from the engineering department might be redeployed to accounting without anyone bothering to delete the AutoCAD software residing on the computer. Later, an audit finds that the computer is being used in the accounting department, but no one knows why AutoCAD is loaded or where the license for it is.

Check documentation and record keeping. Internal auditors can get a sense of how well a company is complying with its software licenses -- and how easily it could defend itself in case of a vendor audit -- by examining how the company maintains its documentation. Brey says that a company should be able to produce its licensing files easily and, ideally, have them centralized, "but sometimes they're scattered and an organization is not even sure exactly where they are all located."

Compare software licensing costs with the number of computers. Another way auditors might spot possible licensing problems is by analyzing software expenses against the number of computers a company has. "If there are hundreds of computers and a very low software expense, that might be an indicator that a company may be buying one copy and making several more," Brey says.

Perform periodic auditing. Once a company has some of these essential practices in place to ensure compliance with software licenses, it still needs to conduct periodic audits to ensure it remains in compliance. In fact, continuing to audit compliance is really the linchpin of the process, Brey says, noting that too many companies centralize purchasing and develop policy statements but then don't follow through by tracking compliance. "They make the assumption that somebody's watching the store," he says. Experts agree that companies should designate someone within an organization to assume responsibility for monitoring and

auditing compliance with license agreements. This responsibility often rests with someone who has IT or auditing experience, or a combination of the two skills.

Although falling out of compliance with license agreements can happen rather easily and often inadvertently, it's not always easy to get back in compliance, Brey warns. "Once you get out of sync and you've got unlicensed software out there, then you really get into a tough situation."

Sometimes companies can take advantage of amnesty periods offered by software vendors or trade groups to bring their organizations into compliance, but even if a grace period is not in effect, Brey urges companies to contact software vendors to purchase additional licenses or take other steps to become compliant.

In addition to purchasing additional licenses if necessary, Jane Disbrow, research analyst for Gartner, says other corrective actions include updating inventories to make them current with employee and organizational changes and redistributing unused licenses. Disbrow advises keeping audit records whether the company took actions to achieve compliance or if the company found it was sufficiently or even overlicensed. "By carefully documenting the results of these internal audits, a vendor may accept these as proof that a vendor audit is unnecessary," Disbrow says.

Although Brey says he doesn't believe many companies are intentionally noncompliant with their software licenses, he acknowledges that it is a prevalent problem. "I can assure you that a large number of reputable companies probably have some software licensing issues somewhere in their organization," he says. "This is not always a No. 1 priority with companies, so it often falls by the wayside."

However, it's not that difficult to remain in compliance with license agreements. "It's a relatively simple process," Brey says. "But it's a process that's got to be followed."

Related resources:

Software compliance resources and guides

Software compliance auditing resources, articles and advice by AuditNet.org.

[Software Management Guide](#) by the Software & Information Industry Association - includes an audit program and controls questionnaire.

Sample [software policies & procedures](#) by the Software & Information Industry Association.

BSA Software Audit Return - [online form](#). The annual Software Audit Return will help you determine your software legality by asking the right questions about the software you currently license.

Auditing software tools

ABC Lan Licensor 3 by [ABC Systems and Development Inc](#)

CentaMeter by [Tally Systems](#)

Express Software Manager by [ExpressMetrix](#)

GASP Audit Tool by [Attest Systems Inc](#)

KeyAudit by [Sassafras Software](#)

License Broker by [System Integrators Inc.](#)

Software Inventory Analyzer by [Microsoft](#)

Additional resources:

[The Business Software Alliance](#)

[The Software & Information Industry Association](#)

*Contributed by the KnowledgeSpace Internal Audit and Risk Management Community.
For more information please visit www.knowledgespace.com. 30 day free trials available.*