Are You Prepared for a Software Audit?

Just the word "audit" is enough to make anyone shiver, and when it comes to a software audit, the reaction is no different. A software publisher can exercise its rights to conduct a software audit to check that a customer is using its products in accordance with the End User License Agreement (EULA). These agreements are signed by customers when the software is installed. The ability to undertake an audit is a legal right, and therefore, not something end user organizations can refuse to do.

If you haven't already been audited—get ready; it's not a case of if, but when. Nearly two-thirds of all U.S. businesses will be audited by at least one software manufacturer within the next 12 months. Typically, organizations that are audited range in size from 200 desktops to 2,000 and higher.*

If you are unprepared, you will:

■ Waste time scrabbling for information on software and licenses

■ Have no prior awareness of potential shortfalls—and no opportunity to rectify them

■ Not have sufficient information to counter any claims made by the software vendor

The net result? It will cost you more.

Yet, according to a recent Quick Poll survey by IDG Research Services**, only one in 10 companies feel extremely well prepared for a potential software audit, while 47% feel somewhat to not at all prepared.

Why are audits important?

A software audit can be either an internal process, executed by an in-house team or consultants, or it can be done externally, by the vendor. If done internally, the results are used by the organization to check what software is installed across the network, how the software is being used and how this usage compares with the entitlements owned by the organization.

An internal audit is important as it gives the organization an opportunity to adjust software usage, reassign unused licenses and proactively manage any shortfall in their own timescale. Waiting for an external audit means asking for trouble. "If the organization is found to be under-licensed on products, the vendor will demand immediate resolution of this shortfall—which ends in unplanned expenditure," notes Matt Fisher, vice president of marketing & communications at Snow Software.

Regardless of how they are done, software audits are typically conducted using an automated inventory tool, which is sometimes also referred to as a "discovery" tool. The tool scans all the relevant devices, such as PCs and servers, to create an inventory of all the software files installed on the target devices.

"The better the inventory solution, the better job it will do of scanning devices and understanding not only what software files are installed, but how these files relate to commercially licensable applications, suites and bundles," says Fisher. A good inventory solution, he adds, will also be able to track software usage over time so that organizations understand not only what software is installed, but whether it is actively being used. If the solution determines there is unused software, it should be uninstalled or re-allocated to other users.

Asset management challenges

Most organizations with an IT department already have some type of software asset management (SAM) tool. But challenges often prevent full utilization. In fact, 36% of respondents to the IDG survey cite a lack of skilled IT human resources to prepare for an audit; 36% noted difficulty monitoring software not located onsite; and 36% reported a lack of SAM best practices knowledge as the prime challenges when preparing for a software audit. Other challenges include difficulty accessing data in various software management tools (29%) and

Less than one in ten feel extremely well prepared for a potential software audit, while 47% feel somewhat to not at all prepared

14% Extremely well prepared
23% Well prepared
25% Somewhat prepared
36% Not very prepared
37% Not at all prepared
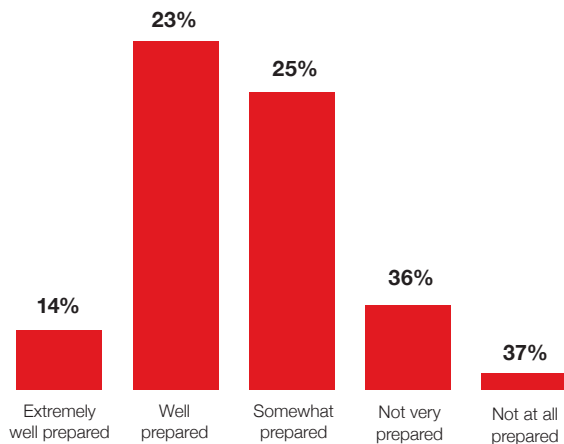
SOURCE: IDG Research Services, August 2013

over licensing of software (22%).

"This is where external service providers can add a lot of value," says Fisher. Indeed, IDG survey respondents cited lower costs and easier or reduced management as the primary attractions of a hosted SAM solution.

How to minimize the impact of an audit

Companies do not have to wait for an audit to occur; they can also conduct self-audits, which are recommended for any organization with more than 150 to 200 PCs. How often they should be done depends on company size, platform and software vendor. For a typical Windows desktop deployment, a bi-weekly or monthly audit schedule should be sufficient, with a quarterly review of the licensing position, he says.

Larger companies that use customized enterprise applications with different licensing obligations should consider more frequent license and usage reviews, Fisher advises.

Many medium-size and small organizations don't take audits seriously until they have gone through a painful "enforced" vendor audit, says Fisher. Unfortunately, not enough medium-size organizations understand that software auditing can also be a proactive way to manage costs—

rather than just a reactive way to address a license shortfall.

How prepared are you?

A company that doesn't use an inventory solution or managed service cannot view the software it has deployed across the corporate network and cannot compare that software to the entitlements it owns. In fact, notes Fisher, most don't know what entitlements they own.

If you're looking to do an internal audit, then the information provided by an audit/license review can lead to savings in a number of areas, including:

■ Harvesting unused licenses instead of buying new ones

■ Cost avoidance by addressing any license shortfalls before an external audit

■ Negotiating more favorable contacts with software vendors

Best practices for software audits

When performing an internal audit, remember to:

■ Cover all the relevant platforms and software vendors—it's not just about Microsoft.

■ Translate discovered software files into commercial applications and suites: You don't license files; you license applications. Good "software recognition" is a must.

■ Audit all devices on the network (and beyond).

■ Consolidate licenses into a single repository—a filing cabinet or Excel sheet won't cut it.

■ Apply intelligence to licensing to understand upgrade and downgrade rights of licenses.

Software audits don't have to be painful. A hosted SAM solution can complement what you are already using and help you make sense of the vast amount of information that is gathered about your enterprise. Not only can you use it as a risk mitigation strategy, but it should also make a strong positive impact on your bottom line.

To learn more, visit
www.cdw.com/sam