CDW PEOPLE WHO GET IT

HOW TO SURVIVE A SOFTWARE AUDIT

Several smart steps can help organizations avoid problems before, during and after an audit.

Executive Summary

Software piracy, whether accidental or malicious, is growing rapidly. Obviously, this situation represents a problem for software vendors as these activities can directly affect the bottom line.

Organizations that use software are affected as well. Along with rising software prices, they can face stiff fines and other costs for noncompliance with software licenses. This can come as a result of an audit that software vendors are more inclined to initiate in a lackluster economy.

It has become almost inevitable that an organization at some point will face a software audit. This white paper will discuss actions to take before, during and after an audit. It will also outline the best ways for the enterprise to remain compliant with software licenses.

Table of Contents

Software Audits Are on the Rise

Even the most responsible organizations likely have unwittingly allowed their employees to use software illegally at some point. That may seem like a startling statement, but it's clearly true. Whether it's on purpose or by accident, the pirating of software is on the rise. According to the *Global Software Piracy Study* conducted by BSA | The Software Alliance, 57 percent of software users admitted to using pirated software – and that's just those who know they are doing something illegal.

According to BSA, the global annual cost of software piracy has reached more than $63 billion. What's more, only 20 percent of software pirates consider current enforcement measures a deterrent to their actions. In fact, 80 percent of software pirates disregard current enforcement measures.

Software noncompliance also occurs when organizations purchase legitimate software copies and then allow additional unlicensed installations. It's easy to understand how this can happen, especially with confusing software licenses, new computing models such as virtualization and the cloud, and the lack of a cohesive software asset management strategy.

The lack of a SAM strategy is a common culprit, says Robert Scott, managing partner of Scott & Scott, a Texas-based law firm with an expertise in software licensing. For example, Scott says, a global company may erroneously assume that its U.S. headquarters office has purchased a global license for a key software product. Based on this assumption, other divisions in the company use the product freely, putting them in direct noncompliance.

Software Compliance: Often Easier Said Than Done

While software license agreements have always been a source of bewilderment, the growing number of confusing clauses and licensing options, combined with new technologies that further muddy the waters, have made software compliance more difficult to achieve than ever. Even a technology refresh or optimization of the environment could cause an enterprise to fall out of compliance.

Among the top reasons why software compliance can be a major challenge for any organization:

- **License rights are increasingly hard to decipher:** It should be a simple matter to read an agreement and understand what an organization is actually getting for the money, but that's not the case. Software vendors can have dozens of different permutations and options regarding license rights, and each has its own idiosyncrasies. What's more, one size doesn't fit all; each software vendor uses different terminology and provides different options. Just because a company finally understands its Oracle license rights doesn't mean that it will understand its Microsoft license rights.
- **Counting is more difficult than 1-2-3:** Both user licensing and access licensing are more complicated than ever. For example, if an organization buys a software license for a server, is that a per-user software license or a per-device software license?
- **Virtualization changes everything:** If an organization has a software license for a server and then creates a virtual instance of that server, does it need additional software licenses for each virtual instance? It depends on the situation and the vendor. One vendor may allow a customer to install an unlimited number of virtual environments on a physical box while others may limit the number or prohibit it altogether. Virtualization is so confusing in the realm of software licensing that an IDC survey, sponsored by Flexera Software, found that 43 percent of organizations don't have sufficient processes and automation in place to manage their virtual licenses, increasing the risk that they will fall out of compliance.
- **Cloud computing adds to the confusion:** While some cloud computing models don't present much of an issue, others, such as infrastructure as a service (IaaS) and platform as a service (PaaS), do because the cloud provider is delivering the service. Software vendors approach cloud licenses differently, so it pays to read the license carefully. Some, for example, charge per processor or core that the software runs on, while others charge per named or concurrent user.
- **The rise of multi-core processors complicates matters:** As servers with multiple processors have become the norm, each software vendor has developed a different way of addressing the issue. Some require licenses for every processor, while others require only one license per server. Knowing what the license specifies is essential to remaining in compliance.
- **Mobility adds to software audit concerns:** While mobile devices deliver great productivity benefits, they present challenges in terms of software licensing. Most enterprise software vendors publish mobile versions of their apps. However, many organizations may not have the licenses in place for all of the devices using a piece of software. Even if they do, it's difficult to track. The challenge is easy to recognize; according to a study on mobile asset management by the International Association of IT Asset Managers. According to the study, nearly 75 percent of IT asset managers surveyed find licensing and management of mobile device assets to be a challenge. An IDC survey found that nearly half of businesses expect to have to change their approach to licensing because of an increased use of mobile devices for work-related activities.

Software Compliance and Piracy Misconceptions

Remaining in compliance can be a juggling act. Many sources offer good advice, but organizations looking to take control of their software assets also must sift through at least as many misconceptions. Here are some of the most common:

MYTH: A software asset management (SAM) tool automatically takes care of all software license compliance concerns. While a software asset management tool will go a long way toward keeping an organization in compliance, it can't operate in a vacuum. As Robert Scott of the law firm Scott & Scott says, "A tool is just a tool." In other words, without the knowledge of how to interpret and normalize the data and then understand what that data means relative to licensing rules, the data itself is not worth much. An effective SAM program also must have executive sponsorship. "There has to be someone in the organization who can write the last email of the stream to drive an initiative like SAM forward," Scott says.

MYTH: Outsourcing software license management is a way to eliminate noncompliance liability. When it comes to software license violations, the buck stops with the enterprise. Even if the outsourcer does a great job managing software licenses, any liability that occurs as a result of noncompliance rests with the organization that owns the hardware and uses the software.

MYTH: Software vendors and BSA are only concerned with auditing large enterprises. While large enterprises are definitely "big fish," this fact does not let small and midsized companies off the hook. In fact, BSA and the Software & Information Industry Association (SIIA) focus much of their efforts on small- and medium-sized business (SMB) audits. An analysis by the Associated Press found that most of BSA's software violation settlements with North American companies came from small businesses.

MYTH: Software piracy is a victimless crime. Even if it's inadvertent, piracy still has an impact. It deflects funds that software manufacturers could use to improve their software and contributes to rising product costs. According to BSA, 19 percent of all business software is unlicensed. Reducing software piracy by just 10 percent worldwide could add more than 25,000 high-tech jobs, about $38 billion in new economic activity and $6.1 billion in tax revenue over four years.

MYTH: Software copy protection makes software more expensive. When software is licensed properly, software developers don't have to raise prices.

MYTH: Software copy protection gets in the way of the legitimate user. With modern software copy protection, this claim is simply not true. Copy protection ensures that the software can't be tampered with, and it doesn't affect performance.

MYTH: Inexpensive software is not copied. While many popular applications are free for private citizens, their use by a business organization can trigger a purchasing obligation. Often, companies simply don't know that because they don't read the agreement. This happens most often with programs such as utilities and accounting software that are free for individual users.

Whether malicious or accidental, software piracy is defined as the unauthorized use, distribution, sharing or copying of copyrighted software. It also includes installing software more times than a license permits, as well as license code, activation key, user ID and password infringement.

Software piracy is illegal and can result in both civil and criminal penalties. In the United States, violation of the *Copyright Act* is a criminal offense and can result in fines of up to $150,000 for each software program pirated or copied.

Software piracy can have other unpleasant effects as well. Unlicensed software can expose an organization to security threats such as malware, ransomware, spyware and viruses.

The increase in the unlawful use of software has spurred software manufacturers to take action. All major software vendors have increased the number of software audits on organizations to determine whether they are in compliance with the terms of their contracts.

Software manufacturers also have found that increasing the number of software audits they perform is an effective way to dampen the effects of a weak economy. The revenue they recoup from audits has helped to fill in the gaps created by a decrease in new license revenue.

The bottom line is that more than ever, the enterprise should expect to be subjected to a software audit. According to Gartner, an organization has a 65 percent chance of being audited. It pays to be prepared.

The Software Audit: What You Need to Know

Many factors can trigger a software audit — everything from routine checks to red flags, such as the use of software on no-name servers or the lack of a SAM program. Another tactic that makes auditors suspicious is quick, surreptitious removal of installed software in an effort to avoid penalties.

When an organization faces an impending software audit, it will receive a formal notification, either from

the software vendor, a consultant hired on behalf of the vendor, or a watchdog group such as BSA or the Software & Information Industry Association (SIIA). While preparing before an audit is by far the most effective strategy — especially because an organization is bound to undergo a software audit at some point — once notice has been received, audit preparation should shift into high gear. Most audit letters require a response within 30 days.

Preparation is critical, yet many organizations are ill-prepared to face a software audit. According to a recent study by Flexera and IDC, less than one in 10 companies feels extremely well prepared for a potential software audit, while 47 percent feel somewhat to not at all prepared.

Before the Auditors Arrive

The first step to take after being notified of a software audit is to contact the vendor to determine the scope of the audit. Depending on the answer, it may be possible to proactively address any shortfalls and circumvent the audit entirely. For example, the scope of the audit may include only certain products, a subset of users' computers, defined time periods or specific locations.

Organizations must clearly understand the type of software audit that is being requested, and which organization is conducting the audit — the vendor, a watchdog association or a third party (usually a public accounting firm). If BSA or SIIA is conducting the proceedings, for example, a formal contractual audit may not be required. The review might instead call for a self-audit, where the software vendor requires the business to create a comprehensive list of the software it uses, along with details about versions, users and hardware. The results of the self-audit determine whether it will be extended into a formal audit.

Once an organization has been contacted about an audit, it should engage an attorney as soon as possible. This should be either an in-house legal team that is well-versed in software compliance or an external firm that specializes in software compliance.

The organization's IT team or procurement specialists should not handle software audits. An audit is a legal proceeding and should be treated as such. Attorneys with experience in software audits know what to say, as well as what should remain unsaid. What's more, software licenses are complex and require specialists.

For example, an IT specialist appointed to head a software audit response team may unwittingly divulge information in a misguided attempt to help. But an attorney will know when silence is in the best interest of the organization.

When the going gets tough, software audit attorneys can provide essential help. With their knowledge of software vendors and the intricacies of licensing agreements, they are in the best position to negotiate the most favorable terms or arrange for license true-ups (in which the software vendor agrees to forego fines if the organization purchases an adequate number of software licenses). An attorney also can help if the process moves toward mediation or arbitration instead of litigation.

It is equally critical to begin an internal software and physical audit as soon as notice arrives of an impending vendor audit. While this should be done routinely, it takes on new significance when an audit is on the horizon. It should be a combination of manual accounting with representatives from all areas in the company and a reconciliation of the company's SAM system and IT asset management (ITAM) program. The audit should compare entitlement, deployment and usage data and review license terms, calculation methods and use restrictions. All of this data should be reconciled to confirm compliance or noncompliance.

An internal audit also should include a physical audit of all active, inactive, stored and remote hardware — everything from desktop and notebook PCs to servers, repositories, backup systems and mobile devices. By mapping the hardware to the software in question, the organization will have a much better idea of where it stands.

Next, create an audit response team, with one person appointed as the point of contact for the audit process. The software audit team should include senior management and representatives from the legal, IT and finance departments.

Finally, negotiate the type of audit that the vendor will conduct, if possible:

- **Self-audit:** This type of audit is performed by the business itself, as directed by the software vendor or trade association. It is generally considered the most favorable option, because the company controls the process, the timing and the resources involved. Self-audit can be part of the pre-audit negotiation with the software vendor.

- **Formal audit:** This can be performed by the software vendor, a trade association or a third-party accounting firm.

Sometimes, a formal audit requires that a vendor enter the workplace to access computer systems and verify compliance status. It's best to avoid this type of formal audit, which can be expensive and time-consuming, and over which the organization has little or no control.

During the Audit

The audit will probably begin with an overview of what will occur during the process. The overview generally will define the scope of the audit, the methodology to be used and compliance criteria. At this point, the organization's attorney goes to work pushing back and setting limits and expectations.

For example, the attorney should make it clear that while the organization intends to comply with requests during the audit, it will only go so far. The attorney should also require a draft of the auditor's report before it is made final to ensure that it is accurate.

During the audit itself, the organization should work hard to manage the process carefully, proactively and aggressively. It must fully understand the audit rights in the provider agreement and push back against any activities that aren't mandated. It also must ensure that all communication is appropriate, documented and validate that the auditor has included all licenses to which the customer is entitled.

The audit team should make certain that the software vendor's claims are accurate. For example, license entitlements may be incorrectly applied, test servers may be listed as production machines and incorrect assumptions may be made around virtual server pools or multiple processors — any of which could significantly skew the audit.

After the Audit

Once the audit is complete, the final step is negotiation. As with other steps, preparation is essential. Before entering any negotiations, the organization should review the final report to ensure that the results are correct and raise any points of contention.

Although some organizations accept the software vendor's edict on penalties, this is a mistake. The settlement always has room for negotiation, so the organization should develop a counteroffer. Software vendors often will strongly consider the counteroffer for two reasons:

1. A fast settlement is in their best interest.

2. Vendors want to keep the company as content as possible to avoid alienating it as a customer. These factors provide some leverage, and it pays to use it.

The audited organization should never sit back and passively accept the vendor's settlement terms, processes and results. In addition to the financial cost, passivity can result in "fishing expeditions" that serve to identify additional violations and increased settlement costs.

A good rule of thumb is to start from a settlement fee based on the estimated cost if the enterprise had stayed in compliance. For example, if the audit finds that the organization is short by 25 licenses, the negotiation should start at the cost of adding 25 licenses.

Don't sell the negotiation process short; it can yield extremely positive results, especially when combined with cooperation. Savvy organizations can negotiate the starting penalty down by 50 percent or more by offering to implement a SAM solution to catch further problems, for example.

What Not to Do When Facing a Software Audit

Organizations that face a software audit should avoid certain actions that can hamper the effectiveness of their response.

- **Don't go it alone.** Software audits are legal matters. Hire a professional.
- **Don't be belligerent.** Animosity is nearly always ineffective. At best, it could lengthen the process, and at worst, it could cause auditors to increase the intensity of their review.
- **Don't be afraid to push back.** It's entirely possible that an auditor may not have considered certain relevant facts, such as past good faith efforts to comply with license rules or past promises made by a vendor.
- **Don't go on a software buying spree to rectify the situation.** Don't think the auditors won't find out about the noncompliance. They will.
- **Don't forgo a nondisclosure agreement.** Insist on enforcing the terms of an NDA, because it can help limit what auditors can do and ask for during an audit.
- **Don't admit or deny allegations of noncompliance.**
- **Don't sign anything that hasn't been approved by a lawyer representing the organization.**

Benefits of SAM

COST SAVINGS: Lower costs are associated with purchasing and maintaining a software library and IT systems.

RISK MANAGEMENT: Control business and legal risks related to improper software deployment. Also lower chances of malware by using a SAM plan to ensure only genuine software is deployed.

SAM ADVANTAGE: Stay ahead of the competition through streamlined operations and faster time-to-market.

GOOD GOVERNANCE: Achieve and demonstrate compliance with your responsibilities under vendor contracts and government legislation.

DISASTER PROTECTION: Protect your company's valuable software assets in the event of unexpected adversity.

Source: Microsoft

Best Ways to Stay Compliant

While software audits are inevitable, organizations can take concrete steps to mitigate the pain and uncertainty that accompanies them. By keeping constant tabs on the software installed throughout the company, who is using it and what hardware it runs on, along with ensuring adherence to the details of the software licenses, organizations can spare themselves a lot of aggravation.

By far, the most effective way to stay compliant is by maintaining a robust ITAM process. This is usually accomplished with an automated SAM tool for keeping track of software assets. An IDC enterprise survey found that 75 percent of companies use an automated software management solution to maintain software compliance.

What's more, Gartner found that organizations that use software audit and license management solutions tend to spend far less time and money responding to a vendor audit when it occurs. Further, the Express Metrix *Software Audit Industry Report* found that in response to being audited, two-thirds of organizations have modified their approaches to IT asset management to include more frequent internal software audits and implementation of new technology to help with license management.

An ITAM process via software management ensures that software compliance is continuously maintained. When gaps are discovered, companies can take the proactive steps of buying additional licenses or uninstalling illegal copies. A good SAM program will diminish audit exposure and potential financial risk, lower security risks from unauthorized software and reduce software costs.

Although the SAM process can be done manually, using an automated tool ensures that nothing is left undiscovered. SAM tools include software metering to monitor peak usage and enforce compliance for concurrently licensed applications. In addition, they keep track of purchasing data such as the number of licenses, purchase dates and prices, invoice or purchase order numbers, and maintenance expiration dates. A SAM tool also will reconcile that information with the software an organization has installed.

SAM tools track software version numbers and installations that are part of different software suites. They tackle some of the thorniest problems in software license tracking today: virtual-to-physical mapping and the increasing use of corporate software on mobile devices.

Advanced SAM tools can keep track of not only which physical hardware is running software, but also which virtual machines are using software licenses. Knowing which physical host each virtual machine is connected to is key to performing a thorough software license analysis. Comprehensive SAM solutions also incorporate elements of mobile application management (MAM) to keep tabs on software installed on all mobile devices used by employees.

One of the most important functions of SAM is maintaining an up-to-date and consistent software inventory. While some organizations still perform these software

inventories manually by visiting each server and PC in the enterprise to catalog the applications that are running on them, this solution is time-consuming and prone to error. A thorough, accurate software inventory is best done as part of a software asset management program.

All software inventory tools provide the basics — a catalog of software running on all devices within the enterprise — but some are more thorough than others. For example, a Microsoft software inventory tool is very thorough but tracks only Microsoft software. This strategy works well in a mostly Microsoft environment, but if the organization employs a wide range of software, an agnostic tool generally makes more sense.

When choosing an automated software inventory tool, an organization should ensure that it can handle the challenges that enterprises face today in keeping track of software running in virtualized and cloud-based environments, as well as on mobile devices. This software is typically very difficult to track, but is subject to the same licensing issues.

Traditional software inventory tools that find software by examining the network looking for software running on live hosts, for example, may not catch dormant or offline virtual images. Tools that use agents (a program installed to collect information) to find software running on specific servers can have difficulty with virtual servers.

Mobility creates a serious challenge when it comes to software inventory. Unless an organization has employed a MAM program, its IT team may find it virtually impossible to know what software an employee has downloaded on his or her device or determine if software licensing and usage policies are being followed.

While it's possible for a stand-alone software licensing tool to manage these situations, it's more common for SAM tools to reliably collect software information from virtual, cloud and mobile environments. And using a SAM tool for software inventory compiles all of the information in one place, making software license management — and ultimately software audits — less painful.

Another important way to remain compliant is by making software licensing a core part of change management. In general, change management is the process of documenting and managing moves, adds and changes. For example, when a PC or server must be taken out of service, change management governs the processes for decommissioning the old hardware and deploying its replacement. Change management should also address the software license implications of such a change. The same is true if an employee leaves the company: Change management should ensure records are updated to reflect that the user license is no longer being used by that employee and is now available, or has been reassigned to a different user. It can also ensure that the organization has enough user licenses available to add another employee.

Another example: A company may be in the middle of a hardware refresh when it gets notice of an impending software audit. How does the company manage its hardware refresh without jeopardizing its legal rights in connection with an audit? An effective change management process will ensure that the organization does not destroy any evidence relevant to the audit and that all changes are documented.

Watchdog Groups: BSA and SIIA

Software audits are such big business that not one but two industry associations are devoted to keeping track of the action. Both BSA | The Software Alliance and the Software & Information Industry Association represent major software vendors, including Microsoft, IBM, Oracle, Adobe, Symantec and Autodesk. Acting on the behalf of their member software vendors, both organizations are alert for situations of software noncompliance. When found, they notify the software vendor, which authorizes a letter requesting a software self-audit by the organization. The results of such a self-audit may lead to a formal audit request.

BSA and SIIA also provide services on behalf of the software industry to protect intellectual property rights through advocacy. They offer a wide array of educational resources and events, as well as strategic consulting.

Both associations operate in many countries, carrying out software compliance enforcement activities. Their efforts are intended to guard against software theft by addressing violations of commercial end-user license agreements, criminal counterfeiting of software and Internet piracy. The associations also conduct extensive research on software piracy and its effects in an effort to guide policy.

CDW: A SAM Partner That Gets It

CDW's trained and certified technology experts understand the intricacies of SAM and can help organizations take a comprehensive approach to deploying a solution that fits their unique environments. Our team of experts includes:

- **Software asset management specialists:** Our certified specialists can analyze your licenses in depth and provide reconciliation services to help you understand gaps between entitled and deployed licenses. They can help incorporate software asset management best practices into your regular systems management tasks.
- **Licensing account executives:** By attending onsite meetings and technology briefings, these specialists review your current environment.
- **Presales systems engineers:** The engineers are always available to answer in-depth software, licensing and technical questions.

For software licensing and asset management support services, CDW provides assessment, planning and design; assistance with evaluating software licensing program options; contract planning and management; configuration management; and onsite software installation and lifecycle support. Our step-by-step approach involves:

- An initial discovery session to understand goals, requirements and budget
- An assessment of the existing IT environment and definition of project requirements
- Detailed evaluations, recommendations, environment design and proof of concept
- Procurement, configuration and deployment of the chosen solution
- Telephone support and ongoing product lifecycle support

To learn more about CDW's software license management solutions, contact a CDW account manager, call 800.800.4239 or visit CDW.com/SAM

Symantec

Symantec Client Management Suite 7.5 powered by Altiris technology enables IT flexibility while empowering employee freedom. The suite helps IT remove boundaries by ensuring systems are securely managed regardless of location, enabling new devices to improve user productivity, and controlling complexity through automated patch management.

CDW.com/symantec

CDW PEOPLE WHO GET IT