Justifying projects in software license compliance

The role of software license compliance within an organization

White paper

Introduction

When most executives think about compliance, their thoughts immediately turn to new financial reporting initiatives. Executives are working furiously to enable their organizations to meet the requirements of U.S. legislation governing the reporting of financial information by publicly traded companies. Another compliance issue, however, also looms. Software license compliance is increasingly a challenge for organizations worldwide. This paper introduces the risks that organizations often unknowingly take by not making software license compliance a priority. It identifies simple policies and processes to mitigate risks through immediate implementation.

Software license compliance—the risk

With very little warning, an organization can find itself a target for a software audit by a software vendor or a software trade association. The risks of such audits are very real and can become expensive if ignored. Every year, software companies and software trade associations conduct thousands of audits. The right for vendors to audit is usually agreed to in standard software license agreements and can be exercised with as little as 30 days notice. These audits can result in heavy fines of as much as $150,000 for each infraction discovered.

According to leading IT industry analysts, the probability of a mid-sized to large organization being audited is approximately 40 percent in the next two years. Analysts also note that audit activity is increasing by almost 20 percent each year.

Most organizations are not knowingly out of compliance with their license agreements. A lack of policies and controls, however, usually leads to practices that place an organization at risk of damaging fines. Organizations should begin to protect themselves from potential litigation and expenses from software audits by developing both policies and processes that mitigate their risks and allow the organizations to focus on business issues rather than compliance issues.

Sources of software audits

Software companies, after suffering from years of stagnant revenue growth, are paying more attention to lost revenues from intentional and unintentional software piracy.

Worldwide, the software industry estimates that it loses $13 billion in revenue each year with the U.S. contributing $2 billion in losses. A study, conducted by International Research and Planning (IPR) and commissioned by the Business Software Alliance (BSA), shows how even a modest and achievable 10-point reduction in software piracy rates globally could create 1.5 million new jobs, generate $64 billion in additional tax revenues and foster $400 billion in additional economic growth.

Studies conducted by several software trade associations, such as the Business Software Alliance (BSA), SIIA and FAST, working in conjunction with independent auditors, have labeled software piracy rates at approximately 25 percent in the United States, 33 percent in Western Europe and well over 50 percent for Eastern Europe.

Audits usually begin when an organization receives notice through a letter from a software trade association such as the BSA or a vendor. The catalysts for the audit are usually not disclosed, but all of the software trade associations and major software vendors maintain web sites where suspected piracy can anonymously be reported. Several recently audited organizations noticed that audit requests came soon after corporate layoffs or other contentious times.

Trade associations such as the BSA and vendors also perform some minor detective work to discover suspected license violations. Using publicly available information or other means, auditors can establish the number of employees at an organization and compare this information to their own license records. Large discrepancies between the two numbers are a flag to an auditor, even though many types of organizations have employees who do not use computers.

Trade associations also run campaigns in certain geographies to call attention to the issue of software license compliance. For example, in the United States, associations have conducted radio and print advertising that promises organizations "amnesty" and "grace periods" for coming forward with their unlicensed software practices.

Firms such as the BSA have reported that they took in more than $11 million from piracy settlements in 1999 and $13 million in 2000. Analysts estimate that the BSA has taken in approximately $40 million in settlements and catches a company out of compliance every working day.

Responding to an audit

Regardless of the source of the audit notification, most software license agreements contain language that allows the vendor or agents for the vendor to conduct routine audits of license compliance. While the language in most license agreements isn't clear on who will conduct the audit or when the audit must be conducted, the auditing vendors usually have rights. It is common for auditors to demand that an audit be conducted within 30 days and that an out-of-compliance condition exists if the organization is found to be more than 5 percent away from compliance with software agreements. In the United States, failure to cooperate with a request from a software vendor or a trade association puts an organization at risk of being sued under Title 17 of the U.S. Code in a Federal Court. Similar copyright laws protect publishers in other countries.

Organizations are usually officially notified of an audit via a letter to the organization's Chief Financial Officer or corporate counsel from an attorney acting on behalf of the software vendor or trade association. The BSA has publicly reported mailing tens of thousands of audit warning letters during active campaigns. Letters typically include an Audit Return Form and request that the organization voluntarily conduct an audit and report the findings. Letters usually begin with the following paragraph:

> The Business Software Alliance (BSA), an association comprised of leading software-publishing companies, has received information that your company may have illegally-duplicated proprietary software products installed on your computers.

Audits, especially those with short notice, can be very expensive. Audited organizations report paying service providers as much as $35 per device during the audit process. If the organization cannot

prove that it had paid for all installed copies of software before the audit notification was received, the organization must pay the software vendor whatever is required to "true up" or be compliant at full retail prices and penalties. Penalties can usually be negotiated with firms such as the BSA, and most organizations prefer to settle instead of going through the judicial process.

When responding to an audit inquiry from the BSA or anyone else, organizations should be extremely careful so that they avoid jeopardizing their own rights, and they should seek legal advice. A strategy of careful and thoughtful cooperation is usually the most economical way to respond.

Organizations should always ask the requestor for more time to conduct audits as most audit requests ask for results in 30 days. Asking for 90 days to conduct the audit is a reasonable request and can help the organization conduct a more accurate and economical audit. Organizations should also be careful to provide information only about the exact software titles that are specified and only for the organization being audited. Additionally, organizations should take care to control the scope of the audit by limiting their audit to the business unit and geography specified in the audit.

Common causes of non-compliance

Most organizations find themselves out of compliance with their software licenses through a combination of inadequate record keeping, ignorance of their license rights and a lack of policies. Common causes of non-compliance include:

- Lack of a documented software license policy for employees to follow
- Lack of centralized procurement or inconsistent procurement practices
- Lack of an asset management software solution
- Failure to perform regular periodic software audits
- Poor contract record keeping
- Over-buying certain server licenses but not purchasing enough client access licenses
- Ignorance of the terms and conditions of the licensing contracts such as dual-use options
- Misuse of MSDN media and licenses
- Re-imaging of operating systems
- Assuming that vendor and reseller records are accurate

Creating policies to avert non-compliance

The first step to avoid becoming out of compliance is to take the issue of compliance seriously and create a set of policies for maintaining software license compliance. Organizations should provide employees with written policies for procuring software, storing proof of purchase and other procedures. Organizations should appoint an individual or group within its audit or compliance group to publish policies and provide guidance for licensing issues. Besides policies for tracking and maintaining compliance, organizations should indicate the seriousness of the issue by documenting the consequences for failing to follow licensing polices. For example, organizations can state:

> Unauthorized Copies. The unauthorized duplication of copyrighted software or documentation is a violation of the law and is contrary to established standards of conduct for [Company Name] employees. Employees, who make, acquire or use unauthorized copies of computer software or documentation will be subject to immediate discipline, up to and including immediate termination of employment.

Organizations often attempt to centralize procurement of their software, but this may not make practical sense. Documenting procurement procedures and policies can be just as effective as a centralized procurement function. For example, maintaining a list of authorized software resellers and other sales channels helps organizations deal with reputable software resellers. Software vendors, for example, have discovered that resellers have illegally duplicated software or exploited some

loophole. Organizations that have purchased licenses from these resellers, even unknowingly, will find themselves out of compliance. Again, providing a list of reputable resellers is the best defense against this common mistake.

Policies should also include the type of license that the organization has negotiated with the software vendor and what type of proof of purchase is required. Even if the procurement function is decentralized, having a policy and procedure for centralizing the collection of proof of purchase in both physical and electronic format helps account for purchases. During a periodic or on-demand audit, a centralized collection of proofs of purchase will quickly enable the organization to determine if it is in compliance by comparing these records to the physically discovered installations. Some organizations assume that they can access purchase records from the vendors or resellers as required for audit purposes. These same organizations usually learn the hard way that some vendors and many resellers have even sloppier procedures than they do and cannot produce accurate and timely records.

Other policies that address common mistakes will also significantly reduce the risk of non-compliance. Common mistakes often occur when employees assume that their organization possesses dual-use licenses for titles installed on their office PCs. Software compliance personnel should publish a list of software titles, and which versions, permit dual use. Employees also often mistake enterprise license agreements with site licenses.

> Enterprise license agreements (ELAs) from software companies are not site licenses. Most software companies commonly grant enterprise agreements, but rarely, if ever, grant site licenses. A failure to understand the difference can lead to a vendor-directed audit.

Software asset management

Policies and procedures are the first step for meeting compliance but they aren't enough to have complete compliance. Software companies and the BSA suggest that organizations implement a software asset management program that continuously provides a set of controls for maintaining compliance.

While implementing a software asset management compliance program may seem daunting, the project is actually very straightforward and can usually leverage existing technologies.

The first phase of a software asset management compliance project is to conduct a physical inventory of the environment. This process usually requires utilizing automated tools, such as Microsoft SMS® and Tally NetCensus®, which may already be deployed. Often, however, these tools collect data in proprietary databases that are not compatible with other discovery tool databases and do not provide much software asset management functionality beyond asset tracking.

In many cases, no discovery tools exist, or they are deemed unreliable. Instead, a manual physical inventory may be required. As periodic audits and spot checks are needed for compliance, industry analysts have advised organizations to implement accurate autodiscovery tools for the entire organization.

Once a physical inventory is complete, the results need to be stored in a central location outside of the discovery tool database. Organizations often start with storing discovered data in spreadsheets or Microsoft Access databases. While this is much better than attempting to utilize discovery databases, simple repositories are usually not able to provide much value beyond acting as a project-based repository.

For example, most software asset management projects require a repository that can be automatically updated from a variety of sources, including autodiscovery tools, manual entry and procurement systems. Other requirements usually include the ability to track all changes to the repository and optionally stage the changes before committing them to the database.

The second phase of a software asset management compliance project is to reconcile the physical inventory with the proofs of purchase. Often this phase is more daunting than collecting the physical inventory, as invoices and other proofs of purchase tend to end up in filing cabinets and closets. An excellent place to start is with the vendors and resellers themselves, but as mentioned earlier, these records might not be accurate. The initial software asset management compliance project will likely require a painful "fire-drill" approach to finding all invoices and proofs of purchases.

By utilizing a combination of policies for storing proofs of purchase and keeping a software asset management repository, proofs of purchases should be centrally stored, regardless of the procurement organization. A central repository of all contract information and proofs of purchase helps the organization instantly determine their license compliance. By running periodic reconciliation processes against the physical inventory, organizations can track their compliance in real time.

The software asset management repository must be flexible enough to not only store data, but assist in providing information beyond simple reconciliation reports. Other software asset management compliance requirements often include the ability to track more detailed contract information, such as reconciling invoices to negotiated license agreements and the requirement to periodically report purchases to Microsoft as part of License 6.0 agreements. Organizations must also track more detailed contract information such as dual-use installs and MSDN installs, requiring manual input into the software asset management repository.

Summary

The penalties for ignoring software license compliance are well documented and should not be ignored. Organizations must implement a set of processes, policies and controls to comply with license agreements; otherwise, they risk a potentially expensive audit.

Implementing license compliance should be a top priority for every organization. License compliance requires a combination of documented policies, physical inventories of installs and proofs of purchases and an ongoing software asset management process can help maintain compliance.

Organizations should immediately begin by developing procedures to store invoices, contracts and physical inventory information in a central repository, regardless of the procurement process. A set of policies for how software can be purchased and from whom must be documented and communicated to all employees. After completing an initial, rigorous, internal audit to determine the extent of the organization's compliance, adopting sound software asset management practices and processes helps minimize audit risks.

For more information

www.managementsoftware.hp.com

4AA0-6566ENW, June 2006

invent