ISG™ imagine your future®

THE SPECTER OF SOFTWARE AUDITS

Assessing Risks and Keys to Preparation

BILL HUBER, MANAGING DIRECTOR

EXECUTIVE SUMMARY

Audits have become an increasing challenge for businesses as software publishers look to the discovery of customer non-compliance with license terms as a major source of revenue. Buyers who lack effective software asset management capabilities face numerous pitfalls and commonly fall out of compliance with current licensing practices. The stakes are substantial, as software publishers can assess multi-million dollar penalties for discovered non-compliance. While most software buyers act in good faith, non-compliance can arise inadvertently or through the behavior of naïve or unscrupulous employees.

In this environment, awareness of the growing risk of software audits and the ability to identify and mitigate specific risk factors and prepare for and respond to a software audit is imperative.

This ISG white paper examines why software vendors are expanding their use of audits, factors contributing to non-compliance with licensing agreements and events that frequently trigger an audit. The author focuses on defining proactive steps executives can take to formulate an audit response strategy built on an effective approach to contracting, licensing and asset management.

WHAT'S DRIVING AUDITS?

Several factors contribute to the growing propensity of software vendors to execute audits of their enterprise customers' license portfolios.

For one thing, the fundamental shift to cloud and subscription-based models is resulting in lower margins (at least for the short term) and adversely impacting revenue performance and the ability of software firms to meet investor expectations. At the same time, revenue from traditional large on-premise deployments is declining.

In this unfavorable environment, the byzantine complexity of enterprise license agreements increases the odds that customers are out of compliance, thereby providing software vendors an attractive opportunity to exploit non-compliance as a revenue source.

CAUSES OF NON-COMPLIANCE

Enterprises fall out of compliance with software license agreements for a number of reasons.

The most common cause is the ease with which buyers can activate additional modules, whether or not they are contractually entitled to use them. In most cases publishers do not "lock" access to additional modules that the organization has not licensed, so any number of individuals at a client organization can easily activate additional functionality or capacity and, in doing so, create a potential liability for their company.

Similarly, software vendors often provide access to new products on a "sandbox" basis to encourage customers to try new features and functionality. The problem is, the products often make their way out of the sandbox to unauthorized uses. Activations, whether intended or not, become discoverable in an audit.

Virtualization initiatives that move workloads around a heterogeneous server infrastructure and cloud-based IaaS, SaaS and PaaS deployments can also run afoul of licensing rights by significantly expanding the number of devices, domains and users defined in software licenses.

Also, with the growth of cloud and "anything-as-a-service" delivery models, contract terms and definitions are changing dramatically, which has an impact on user definitions and terms and conditions regarding usage rights. As a result, reconciling legacy agreements to the conditions of transformed environments presents a daunting challenge.

Similarly, deployments can vary from plan as a result of staffing changes, project work-arounds, process changes or other reasons. Often the definition of authorized uses and users can be confusing and misinterpreted. In some cases, publishers define extended users as individuals accessing data from one software product that captures data from their product. ISG recently encountered an example of this with regard to a procurement tool that "talked to" an ERP platform.

AUDIT TRIGGERS

Within most software publisher organizations, the software audit and compliance practice either reports to or is aligned with the sales organization. This structural approach provides a key insight into publisher behavior. Broadly speaking, software vendors closely monitor customer environments for red flags that signal potential non-compliance. Customers visibly struggling to manage their software assets – for whatever reason – invite closer scrutiny.

The most common specific trigger of a software audit is a customer's involvement in a merger, acquisition or divestment. Enterprises integrating or divesting business units confront organizational disruption, new geographical and legal jurisdictions and haphazard release and acquisition of users and software licenses.

In this environment, widespread compliance violations are common. Moreover, licensing agreements can be very restrictive regarding M&A activities and their implications, creating gray areas that vendors can exploit. Finally, enterprise executives focused on integrating people, processes and products during a merger tend to give insufficient attention to managing software licenses and compliance.

The expiration of volume licensing agreements can also launch an audit. Enterprise Licensing Agreements (ELA) and Unlimited Licensing Agreements (ULA) are structured to incent customers to conveniently purchase high volumes of licenses. The downside is that these

agreements contain fewer apparent reasons to closely manage usage; as a result, customers defer investing in frameworks to track usage and align licenses with users.

The certification process at the end of such agreement is complex, moreover, and clients often inaccurately estimate the number of licenses that will be converted to other structures, along with the associated support costs. In these instances, clients are likely to either overpay for support because they certify at too high a number to cover their uncertainty, or fall out of compliance because they have certified at too low a number, creating a burden to purchase additional licenses and support, along with paying any penalties to resolve the noncompliance.

Another trigger is an outsourcing event, where access to different applications by the outsourcing provider may not be fully covered under the terms of the various license agreements. A full examination of all licenses corresponding to applications that will be accessed by service providers is very complex, and is often rushed and performed superficially due to schedule and financial pressures.

Changes in spending patterns are another trigger, if for no other reason than the publisher's incentive is to protect revenue. Customers raise alerts when they reduce license quantities, opt out of support or other services or determine not to move forward on a planned new purchase.

More specific and tactical audit triggers include whistle blowers – often disgruntled employees or former employees – who report abuses to trade groups such as the Business Software Alliance. In addition, vendors take note when an account loses its internal licensing expertise – specialists in the arcane world of software agreements are rare and their departure often leaves a significant gap. Finally, an account team that finds itself falling short of its sales target at the end of a quarter will often resort to an audit to boost its numbers.

PROTECTING YOURSELF

A strong Software Asset Management (SAM) capability characterized by careful negotiation and oversight of contracts and licenses is the best way to proactively mitigate the risk of noncompliance and develop an effective audit preparedness and response strategy.

From a contractual perspective, expert advice can ensure clarity around definitions of users and acceptable uses (including provisions for potenstial future third-party hosting and/or outsourcing) as well as audit rights, processes and remedies. When budgeting and building the business case for any software, a reserve provision for audit risk should be included as a standard element in the total cost of ownership model and annual budget. From a SAM perspective, an effective program should include clear roles, responsibilities, processes, measures and governance. A key question is whether SAM should fall under IT, procurement, finance or legal to ensure sufficient visibility and sponsorship to protect the company and maximize software investments.

The program should be regularly assessed to ensure that the program is keeping up with changing industry terms and practices. Program funding should be supported by a strong business case, and financial and risk metrics should be regularly reported at a sufficiently senior level of leadership to confirm the ongoing value of the program.

Effective SAM must also take into account the limitations of any asset management and discovery tools that identify assets and track utilization. There is no panacea from a tool perspective, and successful SAM can often require periodic discovery and testing with alternative tool sets. Regular assessments of the environment can identify potential issues such as oversubscription, and proactive actions such as repositioning licenses, removing modules and negotiating additional capacity are often required.

In the event of an audit, professional assistance from an expert advisor who understands the limitations of the provider audit and contract precedent can usually assist in avoiding a significant portion of any cost associated with resolving an audit, potentially saving millions of dollars. A position of "reasonableness" under the guidance of professional defense is recommended. Technology Attorney John Gary Maynard at Hunton Williams describes this as a "Good Citizen" approach that demonstrates interest in seeking a path to a reasonable, fair and appropriate resolution. (Results can range from a determination that the publisher's claims are unfounded and that zero is owed, to a significant but mitigated settlement.)

In summary, software compliance and audits are a major factor in the cost of technology, and need to be given the appropriate level of focus to avoid painful situations. A strong SAM capability is the best way to proactively mitigate the risk of noncompliance. While many companies today lack sufficient maturity to reliably account for all software usage across their company, steps can be taken to enhance SAM capabilities and develop an effective compliance and audit response strategy.

ABOUT THE AUTHOR

THE SPECTER OF SOFTWARE AUDITS: Assessing Risks and Keys to Preparation

BILL HUBER
MANAGING DIRECTOR

Bill is a recognized industry thought leader and has played an active role in helping to create professional standards and best practices. His areas of expertise include IT sourcing, procurement, sourcing strategies, governance, change management, merger Integration and global contracting. In addition to working at ISG, Bill has had experience as the global head of IBM's Sourcing Managed Services and Chief Procurement Officer at Wachovia. Bill was Chairman of the Board of IACCM, (where he currently chairs the Software Working Group), a member of the Board of Advisors for the Sourcing Industry Group (SIG) and a member of the Society of Information Management IT Procurement working group. Frequently quoted in the press, Bill has appeared in *Computer*world, *The Wall Street Journal*, The *Economic Times* and other publications.

ISG™
imagine your future®

ABOUT ISG

Information Services Group (ISG) (NASDAQ: III) is a leading global technology research and advisory firm. A trusted business partner to more than 700 clients, including 75 of the top 100 enterprises in the world, ISG is committed to helping corporations, public sector organizations, and service and technology providers achieve operational excellence and faster growth. The firm specializes in digital transformation services, including automation, cloud and data analytics; sourcing advisory; managed governance and risk services; network carrier services; technology strategy and operations design; change management; market intelligence and technology research and analysis. Founded in 2006, and based in Stamford, Conn., ISG employs more than 1,300 professionals operating in more than 20 countries—a global team known for its innovative thinking, market influence, deep industry and technology expertise, and world-class research and analytical capabilities based on the industry's most comprehensive marketplace data. For additional information, visit www.isg-one.com.

Let's connect NOW...

ISG™

imagine your future®

