Gartner

Research

Publication Date: 2 February 2010 **ID Number: G00174054**

After the Software Audit: Dealing With the Aftermath and Preventing a Repeat Performance

Victoria Barber, Peter Wesche

Software asset managers and others responsible for software compliance should use this research to help them close audits successfully and ensure that the organization learns lessons from the experience. It will help them to prepare for future audits and to rebuild the relationship with the vendor.

Key Findings

- Fewer than 55% of clients receive compliance statements following vendor audits or ensure that contracts are updated to reflect the work done (see Note 1).
- Issues generally arise during audits due to poor data quality for both entitlement and inventory data on the part of both client and supplier.
- Software audits damage the relationship between customer and supplier, and little effort is made postaudit to repair it.
- Clients are experiencing more than one audit a year — repeat audits either by the same vendor for a different product set or by another vendor (see Note 2).

Recommendations

- If the company has no software asset management (SAM) function, build a business case based on protecting the organization from future unbudgeted costs of a similar magnitude.
- Review vendor contracts to ensure that, before the audit is closed and payments are made, the contract is amended to reflect the results with an updated entitlement statement.
- Take urgent steps to review contracts, entitlement and compliance status of products supplied by your top five business-critical vendors, and prepare for any further audits in order to mitigate risk.
- Keep an eye and ear on the market to see who is auditing, and prioritize reviews of their products accordingly.

ANALYSIS

The volume of vendor audits is continuing to increase, with 54% of respondents in a recent Gartner poll having been approached about an audit in the previous 12 months (see "Gartner Polls and Surveys Show an Increase in Software License Audits" for more detail). While vendors are generally positioning these as part of a SAM or cost optimization service, the focus is on revenue generation through the identification of license shortfalls or deviation from usage terms and conditions. Although vendors are unwilling to admit it, their records of client license entitlement are often incomplete (particularly in organizations that have experienced aggressive acquisition), so audit and inventory data may well be reconciled against inaccurate information.

This increase in audits puts pressure on IT organizations that are trying to balance the significant resource requirement of this activity while avoiding disruption to business operations. The overhead of an audit varies depending on the size of the organization, the maturity of the SAM function and the vendor's approach to audits. But all clients can take the opportunity to improve their SAM data and processes as well as their understanding of their software estate.

In addition to formal audits, there is an increase in requests for self-audit (this may be an annual requirement set out in the contract), as well as for ad hoc reports. This research is also relevant to managing these types of engagements, allowing improvements in preparation for any formal audit. Requests for ad hoc reports should be treated with caution, as they may be used by the vendor to establish the value of undertaking a formal audit.

Consider what the major pain points have been during the course of your audit, and put plans in place to address them before further audits take place. The lessons below are general pointers to areas of concern identified by Gartner in discussion with clients, and they provide a starting point for your review.

Lesson 1: Adopt or Improve a Formal ITAM Solution

IT asset management (ITAM) is responsible for the processes that manage hardware and software assets. SAM is a subset of ITAM, with a dependency on hardware asset management, in that software is installed on and assigned to physical devices (either directly or to virtual machines linked to physical devices). Good hardware asset management and overall IT asset management are key to effective software asset management.

Even where there is an existing SAM capability, audits are a significant drain on resources. Following an audit, SAM should work with finance to calculate the internal costs of the audit. This cost, together with license purchase costs and/or any compliance payments, is the total cost of noncompliance. Vendors may also seek to pass on any costs that they, or third parties acting on their behalf, incur during the course of the audit. In many cases, either the contract or the audit request documentation will state that these costs will be borne by the client if noncompliance exceeds 5% of the total license holding. The details of this unbudgeted cost can be used to support your case for any SAM project, resource or tool implementation indicated by the audit output. Review "Update to the Business Case for Software Asset Management" for guidance on how to get buy-in for SAM. If you already have SAM capability in place, review it against the maturity model in "Optimize Software Licensing Costs With Software Asset Management."

Questions

- What were the financial and operational impacts of resources being allocated to the audit (including technical staff, management, chaperones and business colleagues)?

- Does your organization have the internal expertise to deal with all vendor audits? Consider building a relationship with a SAM specialist who can provide the company with additional support and resources to compensate for any skill or knowledge gaps. Remember that any third party engaged by the vendor is paid for by the vendor, reports to the vendor and will be actively seeking issues to exploit.

Example

- Some vendor audits have taken over 12 months to complete. This creates stress and uncertainty, and, in some cases, results in delays in auditors signing off on year-end accounts due to unknown contingent liabilities.

Lesson 2: Improve the Quality of Your Data

Much of the effort during an audit is focused on the gathering and reconciliation of entitlement and inventory (installations and/or usage) data.

Entitlement

The vendor and customer often have very different ideas as to what the customer's entitlement is, in terms of both volumes of licenses and usage rights. Considerable effort can be saved by ensuring that company records are accurate and that agreement is reached with the vendor as to the entitlement prior to any audit being conducted. If this is not the case, any agreement made during the audit, together with details of any additional purchases made as part of the audit settlement, should be formally documented as a contract amendment, with the license management database updated accordingly. An internal process should be put in place to ensure that this data is updated whenever licenses are purchased. Organizations with no existing SAM database and a need to gather entitlement data should start with procurement records and the associated financial systems.

Even when entitlement records are complete, terms are often ambiguous and open to interpretation. Although e-mails or side letters may not form part of the contract, documentation clarifying queries raised prior to the audit should be used to challenge vendor assumptions. Documents provided during the original contract negotiation (prior to signature) could be considered as inducements to sign, while other documentation contradicting the auditor's position can direct responsibility for issues back to the vendor.

Inventory

Audit disputes may arise over the tools and methodology used to identify software deployment and usage. Whether existing tools or those provided by the vendor are used to gather data, it is important to be clear as to how each product is identified and the way in which usage and deployment are measured. Discussions and agreements made during the audit process should be documented as a contract amendment to ensure that there is no dispute in the future as to the validity of the audit results, that documentation is in place for future reference as to the agreed methodology, or that vendors make favorable changes to their license agreements. As new software is purchased, information on software recognition and usage methodologies and metrics should be included as part of the contractual deliverables in order to avoid future ambiguity as to the company's compliance status.

Questions

- Do you know where to find the company's entitlement data, and is there clear documentation as to what constitutes good-quality proof of entitlement?

- Do you know what each vendor requires in terms of usage or inventory data, and can the data be gathered and/or the reports run easily?

Example

- In one U.K. company, a noncompliance of over £10 million identified by auditors was reduced by 60% when an independent third party analyzed and corrected errors in the data provided by both vendor and customer.

Lesson 3: Build a Collaborative Relationship

However strong a client's relationship with a supplier, and regardless of the type of audit, this is a stressful time that puts pressure on both parties. The teams that initiate and carry out the audit are likely to be different from the operational contacts, and the latter may have no knowledge of any audit, particularly if a third-party auditor or SAM specialist has been engaged. Issues that arise during the audit can put a strain on the day-to-day working relationship with the vendor, if there is one, and this needs to be resolved as part of the audit closure process. Negotiating contract clauses to clarify the items that caused issues during the audit, as well as setting the ground rules for future engagements of this kind, can open a dialogue to help get the relationship back on track. It is particularly valuable to include regular contact points in this process, as they have a vested interest in ensuring an ongoing relationship, whereas the audit team may be targeted with one-off revenue generation. Ensure that the sales team acknowledges the impact of the audit, and use any issues or poor practice (such as reinterpretation of license terms) to negotiate concessions on future deals.

Questions

- Do you know how important to your business each of your software vendors is, in terms of annual expenditure, planned investment and business criticality of the products used?

- Can you afford to terminate the relationship with a vendor that has been particularly difficult to deal with? This is a tempting option, but it should be considered objectively. If termination is an option, issues such as migration plans, disaster recovery, and access to legacy data should be considered and planned for.

Examples

- A company whose audit had been particularly acrimonious took the decision postsettlement to systematically remove all that vendor's technology from its organization, as the relationship had broken down irretrievably, and neither the business nor the technical teams felt able to continue to work with the vendor on business-critical issues.

- A vendor that felt the customer was obstructive terminated an audit and issued a notice rescinding the right to use the software beyond the date on which the audit had been due to be completed, citing material breach of contract. Although this course of action is very unlikely, clients should review the contract carefully, take legal advice, and invoke any escalation or dispute resolution clauses in the contract. If necessary, such action should be challenged via the court system.

Lesson 4: Understand the Importance of Contracts

Audits are hard work and divert resources and attention from normal operational activity. It is, therefore, sensible to conclude the audit with a review of any audit clauses in contracts or license agreements. The main vendor contract should be updated with an agreement as to audit

frequency, preferably no more than one per vendor per year, regardless of the number of products supplied by that vendor. Organizations should also retain the right to refuse the appointment of any third-party auditor on reasonable grounds (for example, conflict of interest). We also recommend that vendors be held liable for the costs related to any audit — including any costs incurred by the customer if they are compliant.

Ensure that confirmation of license entitlement at the date of audit, together with a statement of compliance as of the same date and a commitment not to reaudit usage prior to the audit date, is appended to any existing contract or included in any new contract.

In negotiating these points as part of the final settlement, organizations that have demonstrated compliance will be in a stronger position than those with license shortfalls or in breach of the usage rights. However, it may be that inclusion of these amendments to reduce future risk is of greater value to the organization than any negotiated payment reduction.

Questions

- Does your contract confirm your compliance status as of a given date (for example, system go-live or audit closure)?
- Are additional purchases appended to the contract, or is there a statement clarifying what form license entitlement documentation will take?
- Does the audit clause in your contract limit the frequency of audit and require reasonable notice to be provided by the vendor?
- Does your contract state how to identify usage for compliance purposes, and do you have the tools to do this?

Examples

- A vendor carried out multiple audits of one organization within a given year, citing different products and/or different systems to be audited on each occasion.
- Vendors or auditors installed tools on production systems that have caused operational failures on business-critical systems.

Lesson 5: Improve Internal Processes

You are likely to be audited again.

Gartner inquiry indicates that many clients are experiencing more than one major vendor audit a year. Rather than waiting for this point to be proved, start preparing for the inevitable and carry out a review of the organization's top five vendors by operational importance to minimize exposure. Review contracts, validate entitlement and investigate any missing data; research, implement and test audit methodologies; put internal management and housekeeping processes in place to maintain control over these products; and if the opportunity arises (for example, contract renegotiation or renewal, or a significant purchase), amend the audit clause in the contract to reduce the likelihood of frequent audit.

Operational teams within the organization may not see SAM as a priority or have sufficient knowledge of license agreements to comply. Robust processes and effective communication are tools that should be used to ensure compliance and minimize risk.

Questions

- Does everyone in your organization know what to do and who to contact if they are approached by a vendor with a request to audit?
- Do you have a confidentiality agreement or nondisclosure agreement (NDA) in place with both the vendor and any third party that may be performing the audit on the vendor's behalf to ensure that information about your systems and compliance data is not passed on to other vendors with which they may have relationships?

Examples

- Technical staff members, providing data at the request of vendor contacts, have provided outdated or incorrectly sourced data, giving an inaccurate picture of the company's compliance status.
- Staff members, providing the data to vendors, have provided full datasets including commercially confidential information and employee data, resulting in breaches of privacy legislation.

Gartner research during 2009 indicates that the top 10 companies most likely to request an audit are:

- Adobe
- Attachmate
- BMC
- HP
- IBM
- Microsoft (see Note 3)
- Novell
- Oracle
- SAP
- SAS

RECOMMENDED READING

"Findings: Polls and Inquiries Indicate That Clients Should Be Prepared for an Oracle Audit"

"Polls and Surveys Show an Increase in Software License Audits"

"Reduce the Risk of Noncompliance in Case of Software Audits"

"Prepare for an Impending Software Audit"

"Update to the Business Case for Software Asset Management"

"First 100 Days: As Software Asset Manager"

"Verifying Compliance With Microsoft"

Note 1
Postaudit Compliance Statements

In 2008, Gartner started tracking client statements about audit confirmations from its audit-related inquiries in an informal way. Out of a sample of 41 inquiries in 2008 and 2009, only 17 confirmed the receipt of a compliance statement, compared to 29 that received a final written statement as to license entitlement. It shows that vendors provided explicit compliance confirmation in only 41% of the sample.

Note 2
Audit Frequency and Confidentiality

Vendors do communicate with each other, and staff may also move from one vendor or audit company to another. Vendors need to be made aware that any leakage of data obtained during the audit, whether from them or a third party employed on their behalf, will be considered breach of contract, and they will be held liable for their actions. Third parties acting on behalf of the vendor should be asked to sign NDAs and confidentiality agreements in their own right, and they should not expect to be covered by the vendor's existing agreement. The vendor's agreement should be reviewed, and if appropriate, an additional, specific audit-related agreement should be put in place. In addition, a company's own employees may inadvertently alert other vendors to potential opportunities through passing reference to audit activity. Operational staff members need to understand the seriousness and confidential nature of license audit activity.

Note 3
Engaging With Microsoft

In general, Microsoft carries out "SAM engagements," which are intended to be collaborative, and for which Microsoft engages third-party SAM specialists to act on its behalf. The third party will work with the customer to assess its SAM maturity and recommend changes, as well as review Microsoft compliance and the steps needed to rectify any shortfalls in licensing that are identified (see "Verifying Compliance With Microsoft").

REGIONAL HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
U.S.A.
+1 203 964 0096

European Headquarters
Tamesis
The Glanty
Egham
Surrey, TW20 9AW
UNITED KINGDOM
+44 1784 431611

Asia/Pacific Headquarters
Gartner Australasia Pty. Ltd.
Level 9, 141 Walker Street
North Sydney
New South Wales 2060
AUSTRALIA
+61 2 9459 4600

Japan Headquarters
Gartner Japan Ltd.
Aobadai Hills, 6F
7-7, Aobadai, 4-chome
Meguro-ku, Tokyo 153-0042
JAPAN
+81 3 3481 3670

Latin America Headquarters
Gartner do Brazil
Av. das Nações Unidas, 12551
9° andar—World Trade Center
04578-903—São Paulo SP
BRAZIL
+55 11 3443 1509

Gartner