

The ABCs of Surviving a Software Audit

Critical steps to take and issues to resolve when the “gotcha letter” arrives



There are three things that enterprise leaders can be certain of today: taxes and an unwanted software audit in the near future.

Unwanted, of course, but a software audit should no longer be unexpected. The number of software vendor audits has been increasing in the last 10 years now as a means of ensuring full compliance with licensing terms, and, of course, full payment for current software usage. Software is revenue-generating activity for many (though not all) software companies. It is also a means to protect their intellectual property, and vendors guard their rights fiercely – it is the life’s blood of their business.

Why were you targeted for an audit? It may have been a disgruntled employee out for revenge, or a software vendor decided it was your turn, or perhaps an IT compliance agency selected your enterprise as part of a random series of audits. It doesn’t really matter – one way or another, it was your turn. The bottom line is that routine, periodic audits are the only way for software companies to ensure full payment for their intellectual property. Demand letters from software vendors or IT compliance agencies such as the Business Software Alliance (BSA) are inevitable these days. An audit is not a question of “if?” but “when?”

Little surprise, then, that industry analyst Gartner, Inc. recently reported that 35 percent of the companies responding to a survey indicated that they have undergone an on-site, software publisher-initiated audit. That percentage will grow rapidly in coming years, and far too many enterprises are unaware of the deep impact a software audit can have – financially, time consumed, and productivity lost.

Understanding the Risks of Non-Compliance

Before reviewing the steps that need to be taken in the event of an unwanted software audit, enterprise leaders should be aware of the risks involved. There is nothing fun about a software audit and the best an enterprise can hope for is that it is in compliance, so that mostly enterprise time was drained. At worst, an audit may find an enterprise out of compliance, with significant costs in time, monetary penalties, possible third-party legal and IT fees, and potentially additional software expenditures. Unless a company can prove otherwise, the assumption is that every infringement was willful, and penalties of up to \$250,000 in statutory damages can be charged for each infringement. Furthermore, the costs can also include the recovery of the software vendor’s attorneys’ fees under 17 U.S.C. §505 of the Federal Code. In large organizations, these costs can add up to millions of dollars in a hurry.

Beyond the direct financial costs involved, software audits also impact organizations by disrupting the normal flow of business efforts, drawing resources away from meeting the needs of the company’s customers. The financial impact of an audit may include damage to your brand reputation, with additional marketing costs to recover from negative publicity.

Many organizations are blissfully unconcerned about potential audits because they have policies that forbid the installation and use of unauthorized software. What they may not understand is that any enterprise can unwittingly fall out of licensing compliance over time for a variety of reasons – annual changes in licensing rules, software company mergers, true-up clauses in your licensing agreements, the addition or updating of servers, consolidation of architecture, expansion into new geographies, outsourcing, web-enabled applications ... the list goes on and on!

This is why so many organizations have recently invested in IT asset management (ITAM) programs and software asset management (SAM) programs that effectively manage, control and track software assets throughout the enterprise during all stages of their lifecycle. A good SAM program helps organizations remain

The financial impact of an audit may include damage to your brand reputation, with additional marketing costs to recover from negative publicity.

in compliance in the first place, and greatly simplifies the burdensome process of a software audit. However, whether you have a SAM process in place or not, the critical steps and issues to resolve during a software audit remain essentially the same.

The Audit Response Plan

The dreaded, inevitable demand letter from a software vendor or an IT compliance agency lands on your desk. Now what?

To start with the obvious: don't panic, don't ignore it, don't admit or deny the allegations, and don't discard the letter or hope it will go away. Whether you are ultimately in compliance or not, this is not the end of the world ... but you will need help: legal guidance, your internal IT experts, and possibly third-party IT consultants with experience in handling software audits and negotiating favorable resolutions.

Bear in mind that, although relationships between software publishers and their customers is becoming increasingly confrontational, software companies generally want to avoid litigation and ruinous penalties as much as their enterprise customers. Remedies and penalties are always negotiable, especially if they expect your organization to be a long-time, ongoing customer.

Software Audit Action Steps

The early steps for responding to an audit demand need to be taken very quickly, and in many cases simultaneously. The quicker wheels are set in motion, the more prepared an organization will be to effect a positive outcome.

The ten steps you need to take in the event of any software audit are as follows:

1. **Alert your legal team (internal or external), who will quickly respond to the demand letter within the specified time and request more time to prepare.**
2. **Conduct an automated self-audit, if possible.**
3. **Assemble an audit response team.**
4. **Negotiate the type of audit to be conducted: Self Audit, Independent Audit, SAM Engagement, Vendor Audit.**
5. **Conduct a physical self-audit.**
6. **Validate the physical audit.**
7. **Determine a final response strategy.**
8. **Prepare a summary report, indicating level of compliance.**
9. **Negotiate fines, legal fees, and reconciliation, if possible, or prepare for alternatives: license termination, mediation, arbitration, or litigation.**
10. **Take proactive steps to make the next inevitable audit less burdensome.**

Step 1 Alert Your Legal Team

If an enterprise does not have an internal or external lawyer with software compliance audit experience, it should hire one immediately. Audit demand letters usually require a response within 30 days, so there is time to find the right legal expert. Audit targets will need their knowledge and experience because software audits, like software licenses, are legally complex and remarkably arcane. The initial response should come from a company lawyer or outside counsel, usually a phone call to the designated contact to acknowledge receipt of the

demand. Then the lawyer will prepare a follow-up letter to confirm receipt of the audit demand, review any initial agreements made during the first conversation, and nearly always to request more time to prepare for the audit.

An attorney experienced in software audits not only knows what to do, but what not to do. For instance, *never admit or confirm allegations of non-compliance*. This may seem obvious, but even a partial admission of guilt could lead to an attempt to expand the scope of the audit. An experienced attorney will always make sure that the scope of the audit, and the company's response, remains within the limits outlined in the demand letter and covered by copyright laws.

Equally important, experienced legal counsel will usually set the approach and tone of the audit from the beginning. Senior executives are often inclined to dig in and fight, while "nothing-to-hide" IT people sometimes tends to be overly cooperative. Good attorneys and IT compliance experts understand that the best approach is usually a combination of measured cooperation, reasonable negotiation of audit parameters and processes, and quiet preparation for potential negotiation or, at worst, litigation.

Finally, experienced software audit attorneys are familiar with the complete arsenal of **resolution frameworks** that software publishers have at their disposal for enforcing their licensing agreements. On the least acrimonious end of the spectrum are **license true-ups**, in which the software vendor asks the licensee to make good on a previously agreed upon annual updating of their software licenses; and **cease and desist letters**, in which the software vendor promises to refrain from taking legal action if the customer ceases specified infringements or violations. On the other end of the acrimony scale are **license terminations**, **mediation**, **arbitration**, and ultimately, **litigation** – the last of which is very rare. In between the extremes are four types of software audits: **self-audits**, **independent audits**, **SAM engagements**, and **vendor audits**.

An attorney experienced in software audits not only knows what to do, but what not to do. For instance, never admit or confirm allegations of non-compliance.

Step 2 Conduct an Automated Self Audit

The first thing a lawyer will ask for is the facts. Without some knowledge of the merits of the demand letter, legal counsel cannot know how to respond and represent an enterprise's interests. If an organization has an IT asset management (ITAM) program in place and a complementary software asset management (SAM) program, the IT department should use it within a couple of days of receiving the demand letter to determine quickly what specified software is installed and what software is in use, where, and by whom. Although not as accurate as a physical self-audit (automated systems are only as good as the input controlled by their administrators), a quick SAM audit will help the legal team devise an early response to the audit demand.

Step 3 Assemble an Audit Response Team

Whether or not an organization has an ITAM/SAM program in place, the enterprise will need to assemble an audit response team quickly. As legal counsel responds to the audit demand letter and begins contemplating various response strategies, enterprise leaders should waste no time assembling the various disciplines needed to ensure the best possible outcome for a software audit. The software audit team should include the following:

- **Senior management:** For important decisions, either the enterprise leader (CEO, president, etc.) or a designated member from senior management should be directly involved in the audit. Remember, the potential risks and costs could be very high depending on the size of an organization and its readiness.
- **Legal:** As outlined above, expert legal counsel is essential in the event of an audit, and management should make sure that at least one member of the legal team – internal or external – has some experience with software audits.
- **IT:** No lawyer or senior manager can be expected to have a solid grasp of an enterprise's current IT estate, or future IT needs. The CIO and others in an IT department certainly should, and either an internal or external IT licensing expert with experience in navigating the nuances of a software audit is essential. Their expertise is needed not only during the self-audit and reporting processes, but especially during resolution strategy and negotiations. This is where an IT licensing expert is most likely to have valuable historical vendor knowledge and experience in brokering creative compromises and solutions that can save an organization thousands, or even millions of dollars.
- **Finance:** The CFO or someone close to him/her should be directly involved, along with representatives from accounting and purchasing to make sure the self-audit and report are accurate.

Step 4 Negotiate the Type of Audit to be Conducted

Both legal counsel and IT compliance experts should be very familiar with the four types of software audits. Ideally, they should also be experienced at negotiating the type of audit to be conducted, the specific software licenses and installations to be examined, and specific procedures to be allowed during the audit. Neither legal nor IT expertise alone is usually sufficient to obtain the best results – you need a combination of both working together. In descending order of preference, the four types of software audits are:

- **Self-Audits:** Either a software vendor or a trade association acting on behalf of the vendor will request that an organization conduct an internal audit and report the results. By far the most favorable option, self-audits give an enterprise more flexibility in terms of timing and resource allocation, and they remain in control of the accuracy of the final report/summary. If another type of audit is demanded, most enterprises will counter with an offer to conduct a self-audit instead. And regardless of what type of audit is finally conducted, smart enterprises always conduct a self-audit – automated and/or physical – in advance to give themselves a complete picture of the facts pertaining to the audit demands, to help them devise the best response strategy, and to avoid ugly surprises.
- **Independent Audits:** Although many software licenses include the vendor's right to request an independent audit, they should be avoided if possible. Independent audits by third-party accounting firms can be costly and time-consuming, and the enterprise has little or no influence over who performs the audit, how long it will take, or the specific items to be scrutinized. Typically, the vendor bears the cost of the audit unless a licensing discrepancy of more than "X" percent – usually five percent – is found. In that case, the organization not only pays for the audit, but the vendor can usually dictate the price of any additional software needed to become compliant. Penalties are at the discretion of the vendor. The main advantage of this type of audit is the ethical obligation of the auditor to act independently, unlike the next two options.
- **SAM Engagements:** Microsoft is especially fond of this approach, in which the vendor pays a third-party to conduct an audit and report back to the vendor, normally using the targets' installed SAM system. Although typically less costly than self audits or independent audits, SAM engagements are less likely to require the independence of the auditor from the vendor. On the plus side, vendors who request SAM engagements are usually only interested in full compensation for your actual software usage, and will often dispense with compliance penalties if the organization agrees to true-up and remain in compliance moving forward.

- **Vendor Audits:** The least impartial and most intrusive form of audit, vendor-staffed inspections mean granting vendor employees access to your computer network so that they can verify an organization's compliance status. Software publishers often have a legal right to demand a vendor-staffed audit, but it is never wise to agree to one before attempting to negotiate an alternative.

Step 5 Conduct a Physical Self Audit

The largest task of the audit response team is to conduct a thorough physical audit of all active, inactive, stored, and remote hardware – PCs, laptops, servers, repositories, and backup systems – and the software products mentioned in the demand letter. Undertaken as quickly as possible to enable the best response strategy, the physical audit validates and/or corrects the automated SAM inventory, if one was conducted. Very often, the validity of discovery tools such as a SAM program are in question, so a complete physical audit is beneficial, and essential.

During the physical self-audit, the audit response team gathers original copies of all media, certificates of authenticity, and proofs of purchase (current RFPs, POs, invoices, and receipts). In fact, the most important factor in protecting a company's software investment is proof of ownership documentation. Organizations should store the originals in an offsite repository, but copies may be kept in an onsite central repository for convenience. Photocopies of original owner documentation are accepted as valid proof of ownership for audits and usage.

Ownership documentation includes:

- Contracts
- End user license agreements
- Purchase invoices
- Certificates of authenticity
- Bills of lading
- Software boxes (flattened and placed in a labeled storage container)

Anyone who has conducted a physical self-audit knows that maintaining an inventory of all software licensed to the company in a central repository makes it much easier to provide proof of ownership for a complete list of assets in the company's environment. An automated discovery system ensures the updating of inventory data when new software enters the system. It also allows the company to secure the original and backup copies as proof of ownership documents and installation media very quickly and efficiently.

CAUTION: during an automated or physical software audit, it is not unusual for members of the IT department to discover a number of non-compliance situations. Unfortunately, it is human nature to attempt removing installed software from computers on the spot to avoid penalties, but this can be traced easily by independent auditors. One instance of removed software will make outside auditors suspicious, opening the door to a broadening of the audit parameters and more vigilant inspection. Another imprudent reaction to attempt compliance after an audit has been demanded is to purchase more software. Only software purchased before the date of the demand letter is relevant, so this ploy is also imprudent. Management should make it clear in advance that these reactions are not acceptable.

Step 6 Validate the Physical Audit

After the physical audit is completed, audit team members need to compare the documentation with the audit results to ensure they match. This means that each in-scope software matches to a legal copy of proof of ownership, a physical hardware location in the company (hardware, storage facility, RFP, etc.), and a legal copy of installed media.

Step 7 Determine a Final Response Strategy

The first five steps of responding to an audit demand should be completed as quickly as possible, ideally ahead of the timeframe specified in the demand letter. This timeframe is typically 30 days, but can be as little as one week. This is why the legal team almost always asks for more time. An optimal response strategy cannot be formulated until the organization has completed the physical self-audit and validation process, which inform the enterprise of their compliance status, an estimate of the potential financial cost at stake, and their negotiating leverage.

Lawyers and IT professionals familiar with software resolution frameworks must work closely together to determine the best response strategy. Legal counsel will focus primarily on the parameters and processes of the audit, the type of audit, legal rights of the enterprise within the context of the software license terms and conditions, and negotiation/litigation options that range from switching to a different software to evaluating the probability of success based on the facts and a host of relevant legal considerations. IT professionals with software audit resolution experience will leverage their intimate knowledge of software vendor tendencies and focus more on practical compromise solutions that can reduce potential fines and software costs dramatically.

In most cases, the legal and IT teams will arrive at a strategy that combines cooperation, thorough preparation, and negotiation based on:

- The legal facts
- Resolution framework options
- IT-based conciliation/optimization solutions
- The best long-term interests of both the enterprise and the software vendor

Step 8 Prepare a Summary Report

The next step in a self-audit response is a summary of the facts, which the company submits to the vendor or the compliance agency's legal representative. The first goal of this step is written acceptance that the summary is the company's final word and may resume doing business as usual. Therefore, the company needs to ensure this summary is as close to complete compliance as possible. Remember, the greater a company's compliance level, the better their negotiation advantage. Another advantage is the organization's purchasing history, which often enables negotiation of a lower amount than the MSRP the auditor's legal representative will prefer for the non-compliant software products.

In the case of independent audits, SAM engagements, or vendor audits, the company's summary is essential for comparing and/or disputing the accuracy of the outside party's final report.

Step 9 Negotiate Fines, Legal Fees and Reconciliation

A company's preparation and cooperation pays off when it comes to negotiating the cost of potential fines and legal fees. Lawyers familiar with software audits are as prepared to discuss financial options and details as the vendor's representative. A combination of the lawyer's expertise and an organization's cooperation throughout the audit process typically pays off with lower fines and legal fees than those originally indicated in the demand letter, or in the first pass at a settlement. The terms negotiated should include limitations on settlement publicity, providing affidavits from company officers rather than future audits, etc.

A cooperative strategy will also enhance the vendor's willingness to consider IT optimization solutions as a long-term resolution to the dispute. These compromise solutions can reduce potential fines and costs significantly. During a recent software audit of a large corporation by Adobe, an IT consultant was able to negotiate a potential \$3.6 million vendor audit fine down to a little more than \$800,000 – more than 75% – using a comprehensive SAM best practices methodology and proprietary predictive analytics that leveraged enterprise agreements, license optimization, and a reduction of ongoing maintenance costs (request the Animus white paper: *The ABCs of SAM* for more details).

Step 10 Take Proactive Steps to Make the Next Inevitable Audit Less Burdensome

Software vendor audits are inevitable. Considering the potential liabilities of software license non-compliance and the enormous costs in time and money for responding to an audit demand in a short period of time, it should be obvious that an investment in programs, policies, and procedures that minimize ongoing risk are well worthwhile. If the existing IT department does not have the experience to implement these changes, a certified software asset management consultant can help develop policies, processes, and procedures. They can also conduct a test audit and make any changes required.

At a minimum, two programs will help an enterprise maintain compliance while facilitating optimal use and cost of software while protecting against potential disasters:

- **ITAM/SAM:** As a part of IT asset management (ITAM), software asset management (SAM) encompasses the infrastructure and processes necessary to effectively manage, control and track software assets through all stages of their lifecycle. Successful implementation of a SAM program will:
 - o Reduce audit exposure & potential financial risk to the enterprise.
 - o Reduce security risks from unauthorized software within the environment.
 - o Reduce software costs while improving the budgeting process and financial controls.
- **Software Disaster Recovery Planning:** The objective of a software disaster recovery plan is to ensure that an enterprise can recover its inventory data, installation media, and proof of ownership documents in the event of a crisis. This happens to be exactly what is needed in the case of an audit. Similarly, the steps needed to keep a disaster recovery plan up to date also apply to ensuring that the information needed during an audit remains current. Finally, the same thinking that goes into recovering from disasters such as fire and floods also applies to surviving the perils of a software audit. The money saved in the event of disaster is more than enough to justify the cost of a software disaster recovery program; the fact that it also helps organizations survive a software audit doubles the value. With thoughtful planning a company can not only recover from a disaster, it can also have a ready, effective response to a demand letter that ensures the company survives an audit with minimal impact.

What's Your Level of Non-Compliance Risk?

Is your organization in danger of being out of compliance with your software licensing agreements? Before dismissing this threat, or pushing the panic button, enterprise leaders should consider a short list of questions prepared by leading industry consultant Gartner, Inc., to determine if their organization is at a high risk of non-compliance with their software licensing:

- How long has it been since a meeting was held on contract compliance and asset management?
- Does the CIO know who is responsible for IT asset management?

- Are personnel trained in software license negotiation managing the technology contracts?
- Is there centralized technology procurement within the enterprise?
- How long has it been since a desktop audit was performed?
- Are asset management projects funded?
- Does the enterprise have written procedures on software procurement processes?
- Does the enterprise have written policies on software licenses that are not legally procured?

Gartner suggests that if your answer to any of these questions is “no” or “I don’t know,” then your enterprise has a high risk of noncompliance.

A few questions we would add to this list:

- Does your IT department have the tools it needs to maintain a comprehensive view of your IT estate, including software and hardware, to help determine how the software is being used and whether you are in compliance?
- Do you have an effective Software Asset Management (SAM) program in place to help monitor compliance?
- Do you have a good Software Disaster Recovery Plan in place that can periodically update a centralized repository offsite to mirror your onsite software estate?

Again, if the answer to any of these is “no” you should start implementing systems, policies and procedures to protect your enterprise from worst-case audit scenarios. An ounce of prevention can save many pounds of enforced cures.

About Animus Solutions

Animus Solutions, Inc. is a management consulting firm helping organizations solve the toughest enterprise issues and reach their peak performance through the most innovative techniques, processes and technology. Serving both private and public sectors, Animus provides leading industry expertise in areas such as Enterprise Asset Management; Compliance and Risk Management; Change Management; Homeland Security & Emergency Management; IT and Software Asset Management; and Information Technology.



Contact Us:

Animus Solutions, Inc.
Corporate Center One
2202 N. West Shore Boulevard, Suite 200
Tampa, FL 33607

Office: 813-639-7511

Email: phara@animussolutions.com

www.animussolutions.com