Software Vendor Audits

livingstone

a: Global Headquarters - Galaxy House, Unit 3,
Leonard Street, London, EC2A 4LZ

w: www.livingstone-tech.com

e: info@livingstone-tech.com

Contents

Mitigating cost and risk from Software Audits

When it comes to software audits, organizations typically keep a keen eye on the vendors that they spend the most money with. After all, if they are audited by a tier one provider, the financial and relationship ramifications could be significant. Focusing on the bigger providers also makes a great deal of practical sense – Software Asset Management (SAM) teams within organizations tend to be pretty lean, so it is just not feasible for them to stay on top of all vendor relationships. As logical as this approach sounds, it is leaving organizations exposed to a number of audit-related risks.

The impact of an audit stretches further than the settlement fee and these costs are often underestimated or not even considered, even though they are very real and can significantly disrupt an organization's IT roadmap execution by draining financial resources ring-fenced for other important projects.

This eGuide explores activities that trigger audits and the potential risks associated. It includes actionable advice to mitigate the risks, outlines best practices for preparing for audits, and guidance around responding to an audit letter.

Big does not always mean bad

The tier one vendors – IBM, Microsoft, Oracle, and SAP – all have a well-known modus operandi when it comes to auditing their customers' software estates. It pays to be familiar with what they are – then you are in a better position to assess the likelihood of an audit.

Generally, Microsoft is relatively relaxed about its customer deployments, so even if you have invested heavily in its applications, it might not be knocking on your door quite as vigorously as some of the others, and will generally be future focused when it does. Other vendors are hot on some applications, but less so on others; Oracle is a notable example of this. They tend to be more active around their financial year end in May and the Fusion Middleware platform has become a focal point for many of these license audits.

The tier one vendors may be **80%** of the spend and **20%** of the risk, however, the lower tier vendors may be **20%** of the spend and **80%** of the risk!

Smaller vendors can pose greater risks

While companies might spend less with the smaller vendors, in some instances at least, the risk of an audit – and the associated penalties and back maintenance charges that come with them – can be much greater. Indeed, some mid-sized vendors are nothing short of aggressive when it comes to pursuing their audit strategies. They are known to tweak their T&Cs, making audits more likely, more complicated and – most importantly still – more expensive.

Each tier two and lower tier vendor's approach does of course depends on its business culture, but we have noticed a general trend; legacy deployments are more likely to come under scrutiny. It pays to be up-to-speed on their individual policies and behaviour. That way you can get on the front foot.

It is important to check whether the software being used within your company is from vendors included on your approved list. Lines of business – marketing, finance, HR, or any other department – can go 'rogue,' purchasing and using applications without the blessing of IT. This leaves you at risk of being completely blindsided by an audit.

Having visibility of accurate data on your usage and licences for these vendors is important to ensure that they are managed effectively throughout the lifecycle of the contract. Knowing how to use the information this data provides in order to take action and mitigate the risks around audits is vital.

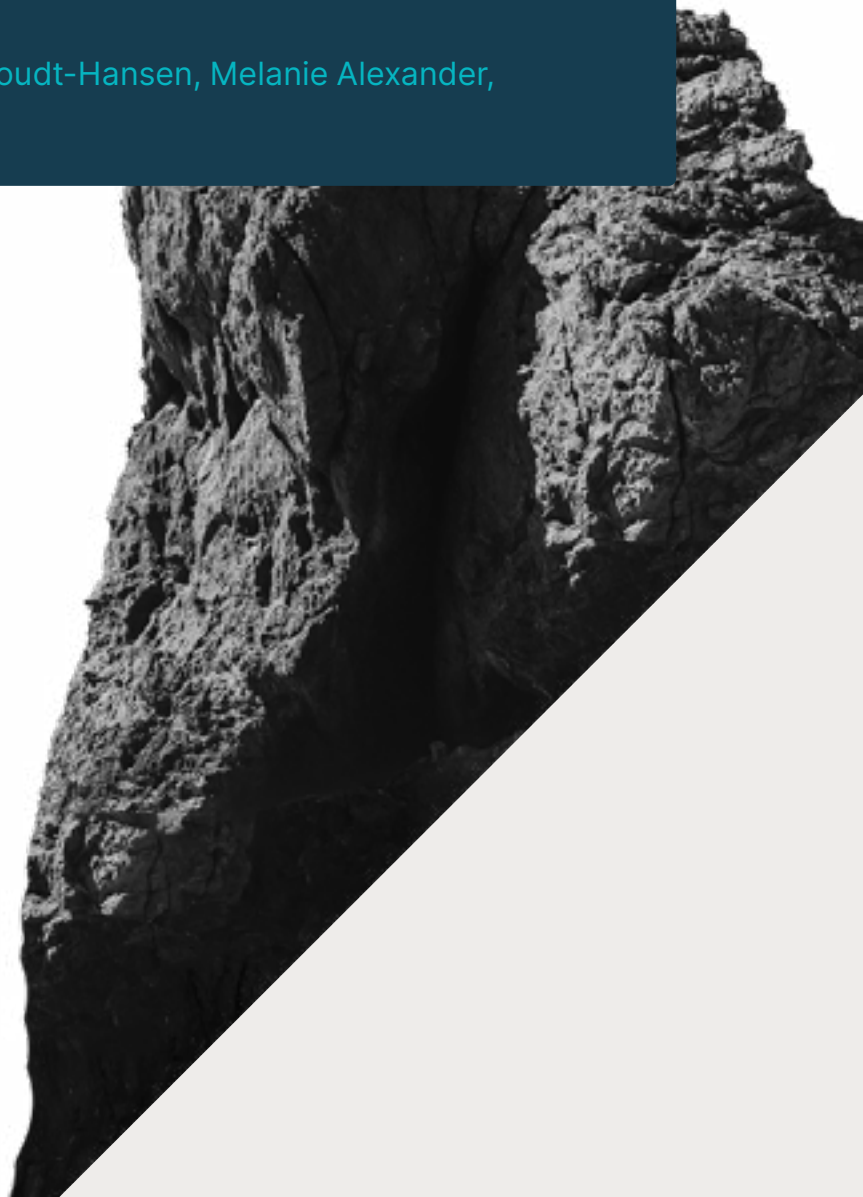
Smaller vendors can pose greater risks

Gartner Report: Negotiating IT Contracts Primer for 2022

Software audit trends vary by vendor. While some curtailed audit activity following a shift to SaaS, others increased compliance audits. Those increasing audits target key scenarios including complexity through hybrid usage, bring your own licence, indirect access, APIs, and storage limits.

Some publishers continue auditing to recover lost revenue or convert legacy perpetual contracts to cloud subscriptions. Minimizing cost and risk of software audits can be addressed by leveraging software asset management (SAM) discipline, evaluating risk, taking control of the audit process through to conclusion and protecting against repeat occurrences.

By Stephen White, Stephanie Stoudt-Hansen, Melanie Alexander,
Published 4 February 2022



Triggers that make audits more likely

There are several common triggers that could spur any vendor to ask to audit your estate.

One of the most common triggers is when an organization terminates a maintenance agreement. Quite often a large part of a vendor's revenue comes from the support maintenance agreements, both renewals and ongoing contracts. This agreement gives the customer rights to use the latest versions of software; so terminating this contract casts doubt as to whether this has been reviewed accurately.

The audit can be used to validate which versions of the software the customer is using and whether they are in fact entitled to do so. As the audit right remains, it can be used to determine whether this support should be brought back to the revenue stream.

Companies that simply renew a longstanding contract, with no tangible change to the number or composition of licences, over a number of years are increasingly attracting attention. Continuously 'pushing back' on the offer of new solutions demonstrates a misalignment to that vendor's strategy.

It's a similar story for companies undertaking digital transformation programmes. Whether they are virtualizing and automating their legacy solutions or migrating to the cloud, there is always a possibility that they might have the wrong type of licences in place. However, refusing to migrate to the cloud may also be a red flag.

Triggers that make audits more likely

Companies investing in professional services from their software vendor are at a heightened risk. While the information these consultants gather should be kept confidential, in many cases we have found that it is seeping back to their colleagues in compliance. A simple support request may leak information indicating misuse or lack of a licence. Some of the more hostile vendors even offer the support team bounties if they can correctly identify a customer ripe for audit. There is also the possibility that the software will "phone home;" alerting the vendor of any suspicious installs or activity.

A breakdown in the working relationship between vendor and client can be another flash point. Perhaps an upgrade or cloud migration did not go as planned, or maybe the client was making unreasonable demands. There may have been a complete move to a competitor's solutions. Either way, an audit could soon follow.

Macro-economic factors are also at play. After the 2008 financial crisis, we saw publishers increase their focus on audits to protect their revenue streams. We can probably expect history to repeat itself as we enter another global recession, as companies rapidly deployed software in order to keep operating during the COVID-19 crisis.

Triggers that make audits more likely

Gartner Report: Do not Underestimate the Total Cost of a Software Audit

Many organizations are blindsided by the sheer size of noncompliance penalties because they are unaware of all the contributing costs. This oversight impedes their ability to properly recognize the risk posed by a future audit.

Sourcing, procurement, and vendor management (SPVM) leaders and IT asset managers should prioritize the software vendors in which their enterprises spend the most, and those that are most critical to business success for a thorough review of the contractual costs associated with a software audit. These risky vendors require extra care when performing normal SPVM and IT Asset Management (ITAM) activities.

By Christopher Dixon, Tobi Bet, Yanni Karalis, Reviewed 2 August 2021, Published 27 February 2020

Mitigate your audit risk

Audits happen for many reasons and it's vital that businesses get proactive, recognizing that it's not a case of if they will be audited, but when. It's important to achieve a perpetual state of audit readiness so that when the letter does arrive, panic doesn't ensue. Whilst many of the audit triggers are unavoidable, there are actions that ITAM/SAM teams can implement to mitigate these risks.

Get familiar with your contracts! This may sound like an obvious place to start but often, organizations will sign up to a contract without proper scrutiny of the terms, particularly, how they will apply in the medium- to long-term. What was right for your company when you signed a multi-year license agreement might not be right now or in the future. Perhaps you accelerated your migration to the cloud to ensure your workforce remained operational during the COVID-19 crisis; does your contract facilitate this? There is a good chance it won't.

We often encounter restrictions around named users, territory and usage by third parties. There are even bigger pitfalls around cloud-based and virtual deployments, product changes and use rights in relation to upgrades, and in hardware and software transitioning, where both are running in parallel.

Mitigate your audit risk

If your contract clauses feel like they are open to interpretation, we have two pieces of advice:

1. Seek independent help from experts with deep knowledge in the contracts issued by the vendor(s) that pose the greatest risk to your operations. They will advise you on each suppliers' modus operandi, so you go into the process with your eyes wide open.

2. Always assume the worst. Vendors use audits to protect their revenue streams, so you can be sure they will try to extract as much value as they can.

Develop a mitigation plan. Implement processes and procedures with solid ITAM Governance and Vendor Management that will outline the way in which your organization interacts with a vendor and the way software is procured and deployed. Publishers are likely to be kinder to non-compliant organizations if they have a mitigation plan in place that illustrates how they will return to a state of compliance.

Vendors will often ask you to deploy an approved reporting tool during the audit, so they can get the information they require first hand, but our advice is do not wait for this – it is too late in the process. Ensure you can proactively supply the data to satisfy the audit. This will help you stay in control of the situation, will provide constant reassurance that you are compliant, and will also give you rich intelligence about your usage, helping you mitigate risk, identify efficiency savings, and optimize your estate.

Before undertaking any IT projects or business transformation, consider the impact and be prepared.

Mitigate your audit risk

Gartner Report: How to Mitigate Cost and Risk During a Software Audit

"By 2026, over 55% of noncompliance findings in software audits will be discovered in public cloud environments. Many Gartner clients report running perpetual software licenses in public cloud environments.

These licences will require an advanced software asset management (SAM) discipline to manage cloud instances to mitigate risk of noncompliance. These public cloud environments have been included as part of the scope of software audits."

By Christopher Dixon, Published 5 July 2022

Responding to an audit

Alongside your mitigation plan it is important for your organization to have a Software Audit Management process in place that defines the step-by-step way in which you will respond. As we discussed earlier, this will be fed with information and learnings from each audit your organization addresses. There are key actions and considerations to include in this plan to ensure the best possible commercial and operational outcome.

Seek expert support

Most organizations will only be audited by each vendor every 2-3 years at most and often, the person responsible for the audit has never engaged with your organization before. This is becoming more the case because of the elevated level of job change we have seen since 2021 and the start of "the Great Resignation".

Engaging with a third party provider is a fantastic way to leverage the knowledge of SAM experts who have provided audit response services for a particular vendor for organizations of all shapes and sizes, understanding the nuances at play.

Go direct

In many cases it can be beneficial to ask your vendor to conduct the audit itself, rather than appoint a third party. This solves issues associated with conflicts of interest and may make the process both smoother and simpler. Even if your contract dictates a third-party auditor can be used, vendors can be swayed, particularly if the customer is large or planning to expand usage.

Responding to an audit

Ask for a deferral

It is perfectly reasonable to ask for a delay if your organization has other mission-critical or time-sensitive priorities making it difficult to free resources to manage complex audit procedures. This was particularly the case for organizations operating in the frontline during the COVID Pandemic - public sector, pharma, logistics or retail, but it is an option available to all companies. The important thing is to follow an audit timeframe that suits your business, not the vendor.

Gather proof

To defend an audit, you will need to provide evidence that your license grant and usage matches the terms set out in your contract. If you cannot provide this information, it will be like a red rag to a bull to your supplier, as they will make worst case assumptions and presume you are non-compliant.

Subject to compliance with all applicable regulations and security policies, the vendor may ask you to deploy an approved reporting tool during the audit if you cannot provide the data required. The outputs or reporting produced by such tools will need to be thoroughly checked for accuracy before they are sent to the vendor. More importantly, they should be analyzed to ensure they only report back on deployments that are within the scope of the of the audit. Very few vendor contracts have requirements to run their tools; assess whether your existing tools will provide the data required. Also bear in mind that some of the data requested may not be relevant to you.

Responding to an audit

Collaborate with other departments

A vendor audit is not – and should never be – the sole responsibility of the ITAM team; engage with other key stakeholders for help. These could be IT buyers or lines of business managers, who must understand the licencing implications of their purchasing decisions. Likewise, the working group should include C-Level, procurement, and finance. It takes a team effort to navigate through an audit, and it is critical that all these stakeholders are aware of the process, and collectively understand what is required and the desired outcome. It's also a good idea to ensure your legal team are aware of any audits, and kept up to date on any that are high risk.

Know your audit rights

Check your contracts to ascertain whether your vendor has the right to review your estate and to what extent. In other words, find out which products and divisions of your organization are included in the scope. Do not presume they can audit everything. Overall, a project and resource plan will need to be put in place and agreed with the vendor before an audit commences, as audit activities will impact the business and the personnel involved.

Find out what information the publisher wants and ensure that by providing it, you are not in breach of GDPR or any other regulations or security policies. Also check the terms of your NDA with the vendor to ensure it is fit for purpose. Some of their data requests may be unreasonable or not required.

It is key that any risky areas are thoroughly understood and mutually agreed before signing off the audit report and before proceeding with commercial negotiations to resolve non-compliance. Furthermore, any future requirements should be taken into consideration, as these may leverage negotiations.

Responding to an audit

Present your mitigation plan

Set out how you intend to remove or redeploy software that is in use, and how you will deal with services associated with people who have since left your company or changed roles. Your mitigation plan should also set out your future usage plans. If the supplier can see you are committed to invest with them in their long-term, they may soften their stance.

Document and evaluate the process

Through the process, record and document each step and activity and learn from it. Understanding what activity triggered the audit is useful. It could be that you were just next on the list but exploring this may provide information that should be included in documented processes. For example, did a conversation with the vendor disclose information?

Apply all the lessons learned throughout the engagement to your Audit Management Process and if you do not have this in place, then use this as a guide to implementing a process to ensure you are able to mitigate the risk of an audit proactively and manage the process more effectively.

Finally, use the data from the audit as a line in the sand and update the information in your SAM system. Moving forward this can be the basis for understanding your organizations needs now and, in the future, and support negotiations for contract renewals.

Responding to an audit

Gartner Toolkit: Optimize Your Software Audit Process and Results

Software audits are inevitable, strain resources and create additional risk if an organization is not adequately prepared. Sourcing, procurement, and vendor management leaders must create a repeatable audit management process in order to minimize their risk and cost.

By Christopher Dixon, Yanni Karalis, Refreshed 30 July 2021, Published 2 April 2020

ST. JAMES'S PLACE
WEALTH MANAGEMENT

Project Managing an Oracle audit to minimize the financial risks

"Not only did we reduce our exposure, the budget we had forecast in our scenario planning exercise was translated into a major cost saving. The team was professional, knowledgeable & collaborative. In short, working with the Livingstone Group was a great experience, with a great result."

Robert Sirignano
Software Asset Manager St. James's Place Wealth Management

livingstone

How Livingstone can help

Our team has experience in managing these complex events on behalf of clients, saving them tens of millions of dollars in the process.

Our services comprise inventory, entitlement, and contract reconciliation to help you understand and reduce your liability.

With expert knowledge on how each publisher approaches audits, we can steer you through the negotiation process and help you achieve the best possible outcome for your business.

To contact our team and discuss your unique audit requirements email info@livingstone-tech.com or visit our Contact Us page.

a: Global Headquarters - Galaxy House, Unit 3,
Leonard Street, London, EC2A 4LZ

w: www.livingstone-tech.com

e: info@livingstone-tech.com