SCOTT
TECHNOLOGY ATTORNEYS

11 SECRETS TO SURVIVING A SOFTWARE AUDIT

INTRODUCTION

With software piracy on the rise, the likelihood that your organization will be audited has also risen.

Flexera and IDC reported recently that less than one in 10 companies are “extremely well prepared” for a potential software audit.

If you’re a medium to large organization using the standard business software provided by the likes of SAP, Microsoft, Oracle, or Autodesk, you can safely assume that:

1. You are on the radar of these vendors or consultants hired by them
2. You are on the radar of the Business Software Alliance (BSA) and/or the Software & Information Industry Association (SIIA)
3. You will be audited at some point in the future

Even if you just purchased a few licenses for 'niche' software with an on-site agreement, compliance needs to be managed. Non-compliance can result in heavy fines.

While a software audit may be cause for some CIOs to press the panic button, being prepared and actively working towards understanding and complying with license agreements is key.

The bottom line? Software audits are challenging but huge penalties are avoidable in most cases. If you know what to expect and prepare for your audit, you have nothing to fear.

In the next few pages, you'll learn the secrets to surviving a software audit so that, if it is due to happen to your organization, you know how to approach it before, during, and after the event.

1. Always respond to a software audit notice

If you're facing an upcoming software audit, you will be informed in writing.

Don't ignore this software audit notice, whether it comes directly from a vendor, the BSA, the SIIA, or another party. Ignoring it is likely to create extra problems or involve litigation.

Audits are serious and won't just go away. Look to respond to notices within 30 days.

Also, note the date at the top of your letter. This is the audit effective date. It is important because this is the date used when the auditor will compare your software deployments to the licenses purchased.

2. Check what the scope of the audit is

Firstly, determine why the audit is happening and what its scope is:

- Who is conducting the audit?
- Does it affect the whole organization?
- Which software is being audited?
- How many computers are involved?

In some cases, a formal audit from an external auditor is not necessary. It may simply re- quire you to detail the use of software with versions/users, etc. in your organization. It's sometimes possible to negotiate this.

In rare cases, it's even possible to take steps that address concerns and fend off the need for an audit entirely.

3. Hire an attorney to work alongside your audit team

You can be sure that the software vendors will use experienced software piracy lawyers. Taking legal advice from the start is essential for you too. As soon as you've been notified of the audit and confirmed its scope, seek legal counsel.

The stakes with software audits are high: too high to be left to IT managers or even CIOs who may not understand all of the complexities of the agreements, the legal requirements, or the legal processes that an auditor will go through.

Being found in breach of software licensing agreements can result in fines of tens or hundreds of thousands of dollars in fines.

If you don't have an in-house legal representative qualified to provide advice in this type of case, engage an attorney who specializes in software compliance.

4. Begin an internal audit

Have your attorney work alongside a team appointed to manage the audit process.

This team should include:

- Senior management
- An IT department representative
- A finance department representative

Once you know you're being audited, it's time to gather as much information about your software and licensing situation as you can.

Hopefully, you already know most of the key points. However, the unfortunate likelihood is that the full software licensing agreements have never been read.

Gartner famously recall one software agreement where the vendor promised a cash reward to any user who signed up. It took months and thousands of sales before anyone claimed!

Bring your own device/application (BYOD/BYOA) agreements with employees complicate

things further.

So, if you've received notice of an upcoming audit, first self-audit to gather most of what you need to know.

In this internal audit, you should:

- Manually audit every piece of software you use in all areas of the organization
- Reconcile your SAM system and IT asset management (ITAM) program.
- Analyze the entitlement, deployment and usage data
- Review license terms, calculation methods and use restrictions for all software packages
- Confirm compliance or non-compliance
- Audit ALL hardware - active, inactive, stored and remote

Avoid the temptation to use free network discovery tools provided by software associations, as the data is often inaccurate. They may even damage your legal position.

At the end of the internal audit, you should have a clearer indication of what the upcoming audit will find.

5. Never attempt to destroy evidence or make knee-jerk purchases

Your audit notice makes it very clear that uninstalling, reconfiguring or purchasing software in response to the audit notice is unacceptable (this is termed a spoiling notice). Treat your internal audit as a snapshot of the present situation rather than an excuse to destroy evidence or "make things right".

It is your duty to preserve evidence and failing to do that will result in more problems if the case goes to court.

The vendor uses expert auditors who will be looking for anomalies. It's another reason to ensure that the process is managed by an attorney.

Purchasing software to "make things right" will only raise suspicion too. Only buy software unrelated to any audit.

Hold off on making any other software purchases until after a complete inventory has been taken.

Then you will have the right to buy or uninstall software at your discretion.

6. Let the legal specialists handle the talking from the start

Before the audit gets underway, the representative of their audit team will usually confirm the scope, explain the processes and methodology used during the audit, and refer to the relevant compliance requirements.

This is where the experience of your in-house legal representative or attorney will come in. Allow them to do most of the talking. Saying the wrong things here could get you into trouble.

Your attorney should:

- Express the intention to comply with the audit
- Set expectations and limits based on what the auditors have expressed
- Request a copy of the draft auditor's report before it is finalized so that it can be checked

7. When the audit is underway, comply with requests but be clear on your rights

After the audit starts, your audit response team (including your attorney) should comply with all requests from the auditors.

Document all communications between your team and their team and ensure that they have included all the relevant licenses for the audited software.

There may be instances when you need to question activities and point out that they are outside the scope of the audit or question the validity of the software vendor's claims or conclusions.

This is best handled by your attorney, who will be fully familiar with your legal rights from the relevant agreements.

8. Understand the penalties and negotiate them

After the audit has been completed and thoroughly checked by your legal representative, it's time to negotiate.

Remember, audit penalties are negotiable.

Software auditors are simply representing the best interests of the software company.

In cases where they find breaches of software licensing agreements, they want to seek the best financial recompense for the organization that they represent.

Often, this exceeds what is acceptable to the party targeted in the audit but the bottom line is that both parties still want to avoid expensive litigation.

The software company usually also wants a rapid settlement and should hope to retain your organization as a customer.

So, before the audit materials are presented to the BSA, ensure you have a full understanding of the financial exposure for your organization with the proposed penalties. Then your lawyer can put a counteroffer to the vendor. Sometimes the penalties can be reduced by 50 percent or more.

9. Fight the legal issues and negotiate non-monetary terms too

A good attorney will be able to force the legal issues at stake in a software audit.

These include:

- What constitutes infringement?
- Who has the burden of proof?
- How should damages be calculated if a shortfall of licenses is found?
- What constitutes proof of ownership?

The financial exposure you face is the main penalty, of course. This can be very one-sided against you.

For instance, the vendor may argue that calculating three times the unbundled MSRP value of the software should be paid in the event of a shortfall of licenses.

This unreasonable conclusion is another good reason for hiring an experienced attorney who will fight your case with the legal issues.

Remember to negotiate non-monetary terms too. These include:

- Future audit obligations
- Confidentiality of the settlement terms
- The nature and scope of the release offered

More about confidentiality in point 11, as it's one of the most important terms to negotiate.

10. Push for "true-ups" if possible

In many cases, a good way to achieve the best result for both parties is through license "true-ups".

This is where the software vendor agrees to forego fines if you agree to purchases the number of licenses that make up for the shortfall.

Keeping it out of court circumnavigates taking legal steps, lowers costs, keeps your organization out of the limelight, and is often a win-win for both parties.

An experienced attorney, seasoned in software licensing cases, will mediate in such cases and push for your best outcome.

11. Ensure confidentiality agreements are in place

Treat the information from the software audit confidentially.

An attorney-supervised audit report is protected by attorney-client and attorney work-product privileges.

If you use outside vendors for IT services, ensure that they have non-disclosure agreements in place before any audit case-related information is shared.

Also, at the end of the audit, ensure that you have a confidentiality agreement (408 agreement) in place with the enforcement agency. Interim confidentiality agreements are normally allowed if the case is pending with the BSA.

These agreements will protect you from software piracy audit materials being disclosed. Without one, you may wake up to a press release naming your company as a target in a

software piracy audit.

Need assistance with a software audit?

Almost all are under-prepared in some way and many underestimate their financial exposure.

Remember that honest errors, such as mistakenly believing that a U.S.-purchased license also covers an overseas office, still breach your licensing agreement and can result in hefty fines.

Ignorance of the software on site is not a defense either. An organization is responsible for all of the software it uses whether it's introduced by stealth or not.

Ongoing and active software license management is the best way to avoid this, of course.

Don't simply rely on the vendor's license management tools as they may end up costing you. Invest in an agnostic license management application.

If you do get audited, adequate preparation is key. Take the tips above on board and you will come out the other side alive and well.

Over the years, Scott & Scott LLP have helped more than 250 organizations navigate the complexities of the software audit process.

To learn more about how we can help you, contact Robert J. Scott via e-mail at rjscott@scottandscottllp.com or telephone at 214-999-2902.

Resources

- www.scottandscottllp.com/top-tips-for-responding-to-an-autodesk-audit/ www.scottandscottllp.com/11-secrets-to-defending-bsa-the-software-alliance-audits/
- https://openlm.com/blog/how-to-survive-a-software-audit-six-step-guide-to-make-sure-you-are-on-top-of-th ings/
- https://webobjects.cdw.com/webobjects/media/pdf/Solutions/Software/145534-How-to-Survive-A-Softwar e-Audit.pdf

SCOTT
TECHNOLOGY ATTORNEYS

CONTACT INFO

Scott & Scott LLP
Suite 200, 550 Reserve Street
Southlake, Texas 76092

Phone: (214) 999-0080
Email: rjscott@scottandscottllp.com

www.scottandscottllp.com