BELTUG Paper

Software Licensing Audits Checklist

August 2015

BELTUG
Be Connected

Why this Checklist?

Software licensing audits are almost always seen as an inconvenience by the targeted organisations. Together with effective software Asset Management however, there are a number of strategies that can help organisations to better manage software licensing audits.

Through technological innovations such as virtualisation, cloud solutions and BYOD, organisations are drastically changing the way software is deployed. An unwanted side-effect of this evolution is that license requirements are also changing fast and therefore the risk of violating license terms and conditions is steadily increasing.

Software vendors make use of this insight by performing software licensing audits to spot check how customers use their software.

This publication explains a number of suggestions that can help organisations how to best deal with an impending software licensing audit initiated by a software vendor.

About BELTUG

With 1200 members, BELTUG is the largest Belgian association for digital technology decision-makers. BELTUG is your trusted interlocutor, to help you to maximize the potential of digital technologies.

We tackle your critical issues and bundle expertise, on both national and international level. We take your concerns seriously and act upon them by talking to the government and the providers. We work on your priorities.

1 Contractual Obligations and the Audit Process

1. Thoroughly analyse the applicable contact terms and conditions to establish the exact audit rights granted to the software publisher. Pay particular attention to the terms and conditions including the non-compliance scenarios. Ideally, this contract analysis should have been performed before agreeing with the purchase of the software licenses preferably with legal assistance specialised in intellectual property rights. If you do not like the terms and conditions then do not buy the licenses and at least try to negotiate changed terms and conditions with the software vendor.
2. Verify and eventually challenge whether the contracted auditor is suitable to conduct the audit. Check the auditor's other engagements with the software publisher and/or your organisation. An auditor that also acts as the financial auditor of the software publisher is unacceptable because of the conflict of interest.
3. In case of an international organisation: ask the software publisher to clearly identify the organisational scope of the audit (which companies, which legal entities). Do not allow the audit to proceed as long as you do not agree with the organisational scope of the audit proposal.
4. Review your company's financial penalty exposure. Some vendors impose penalties and/or charge the cost of the audit to the customer in case of non-compliance. Although non-compliance is seldom by design, it still represents a potential liability.
5. Establish a timetable and clear checklist of deliverables to be produced by the audit, together with the auditor. Do not allow the audit to proceed as long as you do not have an agreement on the audit timetable and deliverables.
6. Ask the software publisher how the audit will be performed and what kind of assistance the auditors will require. Do not underestimate the effort needed to support a software licensing audit.
7. Determine what kind of information the auditor will be given access to and in what form it will be passed on. It is essential that you contractually bind this definition to a non-disclosure agreement.
8. It is highly recommended to only hand over the compliance balance to the auditor and not the underlying raw data.

2 Hardware and Software Inventories

1. Make sure your IT department has a comprehensive view of its entire IT environment, including hardware and virtualisation. This is the foundation for being able to know how the software assets are being used and whether this use complies with the software license terms.
2. Make sure you can easily generate or access a software inventory covering every application installation/change/removal including file and other evidence. This inventory has to be maintained per (virtual) machine included in the hardware inventory.
3. An organisation that does not have its own methods in place to gather information is fully reliant on the information gathering methods and tools of the auditor. These vendor-provided tools perform deep scans into the system configurations, passing on more information than necessary to the software vendor. The use of a license management system would allow the organisation to refuse the use of external scripts and tools, therefore avoiding the risk of the auditor's tools gathering information the company does not want to give to the publisher.
4. As a result of incomplete license portfolio information provided by the software publisher, auditors can mistakenly account for an inflated license demand, and therefore report that more licenses are required than are really necessary. Set up a catalogue on basis of the manufacturer part number (SKU), which contains information about license conditions and rules for

calculating the required number of licenses, making it possible to determine the exact licensing requirements of each software product. Complex license metrics unfortunately require a detailed registration of software license details.

3 Proof of Purchase and License Agreements

1. Always make sure you have a full set of applicable documents ready in case of a software licensing audit. Applicable documents include paid invoices, receipts of purchases, licensing agreements including all addenda and certificates. You should also have access to all soft records of purchases from resellers and software publishers. The list of entitlements is critical to the reconciliation process. Ultimately the most important proof of entitlement are the paid invoices (proof of purchase), not the certificates, the order forms, the serial numbers/keys or other supporting documents. Proof of ownership comes down to purchase records.

4 Licensing Rules and Models

1. Be prepared to demonstrate in-depth knowledge of license types, e.g. device, named user, concurrent user, processor, core based license schemes within your computing environment including virtual machines, multiple processor machines, user groups and sites.
2. Be prepared to demonstrate that the rights of usage and the limitations of usage are understood and correctly applied in your IT environment. This includes the use of upgrade and/or downgrade rights and proper licensing of virtual machines.

5 Software Asset Management

1. Be ready to demonstrate documented corporate policies and procedures used for software asset and license management (hardware and software inventories, procurement, frequent license reconciliation, software download and installation processes, employee awareness programs, internal audits).
2. Put in place an employee awareness and monitoring and control program. Educating employees on what they may and may not install can prevent unauthorized installations and instil confidence with the software vendor. Technically preventing non-authorized users from installing or reconfiguring software is preferable of course.
3. Regularly schedule internal software licensing audits. These internal audits allow you to detect and correct software licensing irregularities before an actual software vendor audit discovers them and will clearly indicate your adherence to IT best practices to both your employees and software vendors.

6 Software Removals and License Purchases

1. Do not start to remove software from computers prior to an audit. These actions are easily traced by auditing companies and in response they will lose confidence in the data presented and start more in-depth investigations.
2. Do not purchase additional software licenses just before an audit in an attempt to cover up non-compliance. In general, only purchases made before the date of audit notification will be considered by the auditors. Additionally, this type of purchase is often seen by the auditors as a red flag indicating a high probability of non-compliance. Also, do not underestimate the possible

domino effect: if significant compliance findings are spotted in your organisation, chances are pretty high other software vendors will start targeting your organisation with additional software audits.

7 Software Asset Management Automation

1. The complexity of software license compliance and increasingly complicated IT infrastructure makes manual management of software assets time consuming and ridden with costs and risks. IT departments should be using automated tools to ensure software license compliance.

8 Typical Danger Zones

1. Virtualisation and clustering: are you aware how many cores/processor units you must count and what the limitations are?
2. Feature limitations: if advanced options are used or a limit of a hardware specification is reached more expensive licenses might be required.
3. Concurrency monitoring: how good is your understanding of concurrency licensing and how well are you monitoring and recording concurrency?
4. Role-based user licenses: role-based user licensing is becoming more common and are often dictated by a user's geographic location, functional requirements, job title and responsibilities within an organisation. Is your software asset and license management system aware of this?
5. Multiplexing and/or terminal servers: are multiple users connecting to a product via a shared account and/or application? Installing an application on a terminal server such as Citrix without setting the correct access restrictions will evidently increase your risk.

9 Conclusion

BELTUG advises its members to be well prepared with good housekeeping and proper software asset and license management to minimise the risk of software licensing audits. In addition to this it will allow the organisation to identify and correct over-licensed applications in which case the organisation can trade-off the cost of running an effective software asset and license management program versus the cost of the licenses saved.

The worst mistake an organisation can make is to underestimate the amount of work an audit requires and to sit back and passively accept the audit terms, processes and results produced by the auditor. Armed with formal audit response procedures, which minimise both organisational disruptions and costs, proactive preparedness is achievable and ultimately the key to a successful audit outcome.

BELTUG vzw/asbl

Knaptandstraat 123 | B - 9100 Sint Niklaas | Tel +32 3 778 17 83

www.beltug.be | info@beltug.be

BELTUG partners