4 Steps to Remove Your Software Audit Stress

Avoiding Frequent Audits

In June 2014 the BSA Global Software Survey, conducted by IDC for BSA, was released. (www.bsa.org/globalstudy) It polled computer users in 34 markets, including nearly 22,000 consumer and business PC users and more than 2,000 IT managers.

The region with the highest overall rate of unlicensed PC software installations in 2013 was Asia-Pacific, at 62 percent. This represented a 2 percentage-point increase from 2011, with the commercial value of unlicensed installations reaching $21 billion!

In separate research, also released by Gartner, the analyst firm states that audits in the twelve months to September 2014 reached an all-time high and that organisations now have a 68% chance of being audited by at least one software vendor (up from 54% in 2009).

As Gartner itself advises, it's not "*whether*" you will be audited by a software publisher, but "*when*".

Scary stuff for organisations with large portfolios and a lack of asset management governance in place. Small organisations are not immune either. In fact, they tend to have less discretionary funding available for unbudgeted compliance incidents, so impact is greater.

And then there's the FAP (Frequent Audit Program) to consider, which occurs when you get your audit wrong the first time, so open yourself up as an easy revenue target. Not something you really want to be known for is it!

So what can lead to an audit?

Here's some common audit prompts:

1. Software vendor suspects you have poor license management, or a poor attitude toward it.
2. A software vendor suspect there is not enough maintenance being paid (especially if there is not a lot of new sales happening with the company or regionally)
3. A software vendor see's company growth without a corresponding increase in licenses.
4. An employee files an anonymous piracy report with the BSA or SIIA. Could be based on ethical ('I know there's pirated software but no listens!') or disgruntled ('I didn't make my bonus again.')
5. A merger or acquisition has occurred. The acquired company may be out of compliance, which was ignored during the 'Due Diligence' process.
6. The infrastructure technology has changed without addressing the change in license conditions e.g. use of BYOD, Cloud systems etc.

Take the Initiative

Gaining control of your compliance is a simple matter of governance with support from the executives. The following is a short generic list of items you should consider to minimise the impacts of an audit being mindful that each organisations maturity, resourcing and attitude is different:

- **Plan for an audit**

- **Fail to plan, plan to fail** – Spend time pulling a plan & checklist together before you need to. The plan should encompass the process, tools, policies and prioritise likely risk areas. This will ensure all aspects can be covered without the stress and urgency.
- **Get control of your hardware** – Software sits on hardware generally. You will need to first get control of how its purchased, where it is, use, storage disposal etc. This is key in managing the software. (We will discuss this in a separate post).
- **Organise resource** – Organise the response team with brief and educate key people, ensure the tools are identified and tested, and the reporting is in place.

- **Review your contracts**

- **Gather the data** – Gather, collate and understand each contract you have with the vendors. This may require some discrete queries should some contracts not be located, seeking an update on the current license position. The data should be input to a contracts or document database system for future access is not already there.
- **Identify rights numbers** – Pull together the actual rights numbers per license you own taking into account which licenses are machine, user, CPU based etc. This data should be input into your asset management system for future use.
- **Gather Proof of Purchase** –Each license must have a proof of purchase identifying you legally purchased the rights. Certificates of Authenticity must be gathered where applicable. This data should follow the license rights for each of extraction when required.
- **Engage a license specialist** – A license specialist should understand the definition of the contract, audits etc. and generally has a good relationship with the vendor organisations. They can also help to unravel the complexity of licenses due to the almost continual change seen from the vendors.
  Bear in mind many local organisations use external specialists who earn bonus's and commissions from the sale of software. And they may be obligated to trigger audits.
- **Clarify contract definitions** – This would include what comprises an install such as file/files, the grant, who is authorised to perform the audit, how it may be conducted, tools that will be used etc.

- **Plan a response**
  - **Who responds** – Clarify who should be receiving the audit letter and who will respond. This should be the legal department.
  - **When** – A response is required back to an audit letter, it cant be ignored. Walk through the various responses to the differing types of audit letters and what they mean.
  - **Clarify what is sought** – Identify items that are unclear from the current contracts. This is an opportunity to move the audit to your favour if done correctly. Time frames should also be clarified.
  - **Clarify tools** – The accuracy of audit tools should be confirmed. You may need to test auditors tool on a sample of devices to ensure the results are accurate.

- **Carry out compliance checks – Self audit**
  - **Gather install/use data** – This normally comes from an inventory tool/s (multiple may be needed depending on the environment). Remember to manually audit those

devices that are not able to be automatically audited. And audit the right files/applications based on the definitions previously collated.

- **Compare rights to use** – The data sources are combined to allow a common view of rights against use. This data is made available through a reporting mechanism.
- **Confirm purchase history** – Reporting of purchase history against rights needs to be reportable too. This data is made available through a reporting mechanism.
- **Produce reports** – Produce a series of reports that show the current state of compliance. These need to be simple, accurate and repeatable.

At this point you have a repeatable and sustainable process for identifying what has been purchased, how many, where their used and what the differences are. Allowing for number growth and shrinkage, the accuracy of your license compliance should now be auditable by any of the vendors with minimal financial, security and organisational risk.

To hold this altogether you must also implement the following:

- **Educate staff**
  - Especially the technical staff on what they need to be aware of, including the legal aspects. This will generally require some level of culture change as most organisations have ignored this requirement in the past.
  - Define piracy and the types, identify risk points within the organisation and seek mitigation.
  - Ratify the policy and compliance management process as it applies to your organisation.
  - Ensure SAM requirements and policies are included part of your induction.
  - Keep policy updated and enforceable (through HR).
  - Provide an ongoing education program using various media available within the organisation.

- **Train the team**
  - Identify and train those who will manage the SAM processes and reporting going forward. The IAITAM CHAMP/CSAM courses are a must.
  - Ensure there is a career path for progression in the organisation.

- **Continuous Improvement**
  - Put in place a continuous improvement program. Don't let the program become a one off exercise.
  - Review and update KPA and KPI's to ensure improvements can be shown over time.
  - Communicate savings made and risk reductions identified to senior management.

Benefits to You

- **Cost Savings -** Understanding what software you do and do not need means you can focus expenditure only on those titles needed for your business. This also allows better deals with vendors in cost and license program options.

- **Operational Improvement** – Better control of software means support is focused on the right products. This in the areas of deployment, removal and application support./ Network and security requirements are easier to manage too.

- **Risk Management** Business and legal risks can be better controlled and more focused by running a good pre-audit program.. You also lower chances of malware afflictions when your program ensures only genuine software is deployed.

- **Good Governance** - Achieving and demonstrating compliance with vendor compliance and government legislation reduces the chance of joining the FAP (Frequent Audit Program).

After all, why would a vendor focus on an organisation who they know has all their ducks in a row!

- **Disaster Protection** – Fire, flood, earthquake and technology 'challenges' can require quick recovery and authentication of software. A good SAM practice ensures software DR impacts are minimised.

So There You Have It

Software Asset Management forms part of the overall IT Asset Management program. It is seen as the sexy cousin to hardware asset management as tangible costs can be readily recovered. However, it relies heavily on having good hardware management in place as part of an overall IT asset management practice in order to provide the financial return.

SAM doesn't need to be a burden, expensive and definitely cant be ignored. When included as part of the ITAM Program, it helps by reducing IT budgets by up to 30% according to Gartner and IDC. Which is great for the business and shareholders alike!