IS AUDIT BASICS

Auditing Software Licenses

Do you have something to say about this article?

Visit the *Journal* pages of the ISACA® website (*www.isaca.org/journal*), find the article and click on the Comments link to share your thoughts.

https://bit.ly/2n0I5QD

Those of you who have read my bio are aware that in addition to writing for the *ISACA® Journal*, I am also a topic leader for the Audit and Assurance community on ISACA's Engage Online forum.[1] A recurring request on the forum is for a software licensing audit/assurance program. This strikes me as something that would be suitable for collaboration and the development of an open-source audit/assurance program.[2,3] However, for various reasons, mostly around a suitable platform, this has not yet managed to get off the ground. Perhaps I have been too ambitious.

I, therefore, propose a simpler approach. I will run through my thoughts on software licensing and ask you, the reader, to add your thoughts in the comments section. In this way we can produce a collaborative audit/assurance program. As in previous columns,[4] I will use the ISACA® white paper *Information Systems Auditing: Tools and Techniques, Creating Audit Programs*.[5]

Determine Audit Subject

The first thing to establish is the audit subject. What does a software license mean in your enterprise? If there are distinct types of software licenses (**figures 1, 2**) in use, it may make sense to record these as separate audit universe items. This is because there may not be the same need to audit "free" software (**figure 1**) as opposed to purchased software (**figure 2**). In addition, where types are the same, the inputs to calculate the license costs will be the same.

The key is to use the guidance to consider the software licenses in use at your enterprise and to determine the audit subject(s). You need to answer the key question: What are you auditing?

Define Audit Objective

Once what is to be audited has been determined, the objective of the audit needs to be established. Why is it being audited? From an auditor's perspective, it is advisable to adopt a risk-based view and define the objectives accordingly. Likely risk factors include:

- Financial (i.e., penalties, fines)
- Reputational
- Opportunity costs

Audit objectives should also correspond to goals as defined by the enterprise (**figure 3**).

Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CIPM, CIPP/E, CIPT, CPTE, DipFM, FIP, ITIL Foundation, Six Sigma Green Belt
Is the group IT audit manager with An Post (the Irish Post Office based in Dublin, Ireland) and has 30 years of experience in all aspects of information systems. Cooke has served on several ISACA® committees and is a past member of ISACA's CGEIT® Exam Item Development Working Group. He is the topic leader for the Audit and Assurance discussions in the ISACA Online Forums. Cooke supported the update of the *CISA® Review Manual* and was a subject matter expert for the development of ISACA's CISA® and CRISC™ Online Review Courses. He is the recipient of the 2017 John W. Lainhart IV Common Body of Knowledge Award for contributions to the development and enhancement of ISACA publications and certification training modules. He welcomes comments or suggestions for articles via email (Ian_J_Cooke@hotmail.com), Twitter (@COOKEI), LinkedIn (*www.linkedin.com/in/ian-cooke-80700510/*), or on the Audit and Assurance Online Forum (*engage.isaca.org/home*). Opinions expressed are his own and do not necessarily represent the views of An Post.

Figure 1—Free Software License Types

Type	Description	Examples
Open source	The software may be used, copied, studied, modified and redistributed as required. Open source is usually accompanied by the program source and a copy of the software license (e.g., the GNU General Public License).	Operating systems
Freeware	The software is free, but the source code cannot be redistributed.	Desktop tools
Shareware	The software may be free initially; however, this may only be on a trial basis or have limited functionality compared to the full, commercial version (may also be known as trial version, demoware or an evaluation copy).	Desktop tools

Source: Adapted from ISACA®, *CISA Review Manual, 27th Edition*, USA, 2019

Figure 2—Paid Software License Types

Type	Description	Examples
Per central processing unit (CPU)	Depends on the power of the server, specifically the number of the CPUs; could include the number of CPU cores	Databases
Per seat	Depends on the number of unique users of the system. Really a subscription for each user.	Software as a Service (SaaS)
Concurrent users	Depends on the total number of users using the software within a predefined time period	Enterprise Resource Planning (ERP) Systems
Utilization	Depends on how busy the CPU is or the number of users that are active at any one time	Database add-ons
Per workstation	Depends on the number of individual workstations (not users) that connect to the software	Desktop tools
Enterprise	Usually allows unlimited use of the software throughout an organization without the need to apply any of the rules above, although there may be some restrictions	Desktop software

Source: Adapted from ISACA, *CISA Review Manual, 27th Edition*, USA, 2019

Figure 3—Business Risk, Enterprise Goals and Audit Objectives

Business Risk	Enterprise Goal (EG)	Audit Objective
• Financial (penalties) • Reputational	• EG02 *Manage business risk* • EG04 *Quality of financial information* • EG07 *Quality of management information*	Review controls to prevent under-licensing
• Opportunity costs	• EG02 *Manage business risk* • EG09 *Optimization of business process costs*	Review controls to prevent over-licensing
• Financial (fines) • Reputational	• EG02 *Manage business risk*	Review controls to prevent the installation of pirated or cracked software

Unusually, for an audit, it is also worth considering what is not an objective. It is not, in my opinion, an objective of a software licensing audit for IT audit to scan the network or otherwise confirm the number of software installations. This, most definitely, should be performed and is a key input to the audit; however, it should be a separate management exercise subject to an independent, separate audit of software or IT asset management.

Attempting to identify all instances of installed software, especially in an environment where there is no predefined scanning, inventory or discovery tool, will result in drowning the audit in a sea of false positives. If it is determined that this is the case, the audit should be stopped and this should be made the key finding.

Enjoying this article?

- Read *Software Audit/Assurance Program. www.isaca.org/software-audit-assurance-program*
- Learn more about, discuss and collaborate on audit and assurance ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Set Audit Scope

When the objectives of the audit have been defined, the scoping process should identify the actual software licenses that need to be audited. In other words, what are the limits to the audit? Examples of scope limitation could include:

- Licenses that are calculated in a similar manner (as previously mentioned)
- The top-five vendors based upon annual licensing cost
- Areas where there is a high likelihood of noncompliance (e.g., after a merger or acquisition)
- Vendors who have recently changed or adjusted their licensing model

Perform Preaudit Planning

Now that the risk factors have been identified (**figure 3**), they should be evaluated to determine their significance. Conducting a risk assessment is critical in setting the final scope of a risk-based audit.[6] The more significant the risk, the greater the need for assurance.

> "THE MORE SIGNIFICANT THE RISK, THE GREATER THE NEED FOR ASSURANCE."

The assurances considerations for software licensing can be grouped by borrowing the functions from the US National Institute for Standards and Technology (NIST) Cybersecurity Framework (CSF):[7]

- **Identify**—Is there a central register detailing the software license entitlements? Does the enterprise record and know the costs of the licenses?
- **Protect**—Does a policy exist for software licensing? Are all licenses centrally authorized? Is all other software strictly forbidden?
- **Detect**—Is there a need for continuous and periodic monitoring?
- **Respond**—Are the results of the periodic monitoring reported to senior management?
- **Recover**—Are corrective actions in place?

Finally, the auditee should be interviewed to inquire about activities or areas of concern that should be included in the scope of the engagement. Once the subject, objective and scope are defined, the audit team can identify the resources that will be needed to perform the audit work.[8]

Determine Audit Procedures and Steps for Data Gathering

At this stage of the audit process, the audit team should have enough information to identify and select the audit approach or strategy and start developing the audit program.[9] There is now enough information to decide what documents are expected for review, what licenses apply, the criteria and whom is going to be interviewed. However, the testing steps need to be defined.

In previous columns, at this stage, I have introduced an ISACA audit/assurance program and documented how the assurance considerations map to audit testing steps. However, ISACA currently has no specific audit/assurance program for software licensing (although the COBIT®-related Build, Acquire, Implement [BAI] BAI09 *Manage Assets Audit/Assurance Program*[10] does provide some coverage and is worth consulting). I, therefore, propose to map the assurance considerations directly to high-level control tests (**figure 4**). I am asking that readers collaborate by adding any missing control tests or observations in the comments section.

Conclusion

The fact that I author this column does not, by any means, mean that I have a monopoly on audit experience. I am certain that I have missed something that others have come across, besides which the editor is hawkish on the space allocated to me. I am, therefore, asking all readers to collaborate by adding their thoughts to the comments section. I hope that this is the first of many such partnerships and that this will become the *de facto* audit/program for software licenses. Alone we can do so little; together we can do so much.[11]

Figure 4—Assurance Consideration to Control Tests Mapping	
Assurance Consideration	**Control Test**
Identify	Confirm there is a central register of all software that is officially licensed by the enterprise. Ideally, this should be linked to an IT asset register and include the: • Name, platform and current version(s) of the software • Contract • Business owner • License type(s) and the evidence the vendor requires to confirm compliance • Number of licenses purchased • Number of licenses in use • Computers (servers and clients) where the software is installed • Date purchased Confirm there is a hardware asset register of all computers and that it is up-to-date and accurate. This should include the: • Make and model of the server/client • Number of processors • Number of cores
Protect	• Request and review the operating procedures and policies for license compliance, including those for any continuous and periodic monitoring. • Request and review procedures and policies relating to installation of pirated or cracked software. • Confirm who is responsible for software licensing.
Detect	• Confirm the use of endpoint management, scanning, inventory, discovery tools or other software or scripts that will detect new servers and clients and the software installed on them. • Confirm that there is a method to detect software licenses where software is not installed (e.g., the number of users for a SaaS). • Confirm that the above are continuously and periodically summarized and compared to the central register of software licenses. • Spot check a sample of the software licenses for a sample of clients, servers or users. Confirm the monetary calculation of the license liability. • Confirm whether the process would likely meet vendor evidence requirements. • Confirm whether there is a mechanism to detect pirated or cracked software. • Analyze whether monitoring techniques for continued compliance follow specified policies and operational guidance. • Confirm that there is a method to detect software licenses in use in the cloud
Respond	• Confirm whether the software licenses are under- or over-licensed. • If under-licensed, analyze the cost of the exposure. • If over-licensed, estimate the opportunity cost. • Evaluate the security methods in place to ensure the proper protection of copyright agreements, licensing agreements and monitoring methods.
Recover	• Determine what corrective actions are in place when under- or over-licensing is detected, for example: – Additional licenses are purchased – Excess licenses are exchanged or contracts renegotiated – Movers, leavers are removed – Software is uninstalled • Spot check and confirm that corrective actions have been implemented.

Endnotes

1 ISACA® Engage, Audit and Assurance, *https://engage.isaca.org/communities/community-home/digestviewer?communitykey=b4f0c214-8b78-4359-8bd0-8f0e7382b68a&tab=digestviewer*

2 Cooke, I.; "Audit Programs," *ISACA® Journal*, vol. 4, 2017, *https://www.isaca.org/archives*

3 Cooke, I.; "Innovation in the IT Audit Process," *ISACA Journal*, vol. 2, 2018, *https://www.isaca.org/archives*

4 *Op cit* Cooke, "Audit Programs"

5 ISACA®, *Information Systems Auditing: Tools and Techniques, Creating Audit Programs*, USA, 2016, *www.isaca.org/Knowledge-Center/Research/Documents/IS-auditing-creating-audit-programs_whp_eng_0316.PDF*
6 ISACA, *Audit Plan Activities: Step-By-Step*, USA, 2016, *www.isaca.org/Knowledge-Center/Research/Documents/Audit-Plan-Activities_res_eng_0316.pdf*
7 National Institute for Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, USA, 2018, *https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf*
8 *Op cit Audit Plan Activities: Step-By-Step*
9 *Ibid.*
10 ISACA, *BAI09 Manage Assets Audit/Assurance Program*, USA, 2014, *www.isaca.org/Knowledge-Center/Research/Research Deliverables/Pages/Build-Acquire-and-Implement-Audit-Assurance-Programs-1-10.aspx*
11 Quote Investigator, Helen Keller, *https://quoteinvestigator.com/2014/04/21/together/*