Audit Programs

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.

http://bit.ly/2rWOyL8

It was a great compliment, if somewhat daunting, to be invited to follow in the footsteps of Tommie Singleton and the late Ed Gelbstein to contribute to this column. I can only hope to match their insights by bringing my own experiences to bear.

Speaking of which, one of the most common requests I get as a community leader on the ISACA® Knowledge Center[1, 2, 3] is for audit/assurance programs or sources of assurance. So, what are our options and where should we look?

Utilize Existing Audit/Assurance Programs

ISACA, the Institute of Internal Auditors (IIA) and other organizations have developed programs (**figure 1**) that address commonly audited areas such as cyber security, commonly utilized applications such as SAP and common requirements for compliance such as the Payment Card Industry Data Security Standard (PCI DSS). These are excellent resources and can save a lot of time. My only word of warning is that they are not one size fits all. They should be considered a starting point and adjusted based upon risk factors and criteria that are relevant to the organization you are auditing. Failure to do so can result in a checklist approach that can lead to the auditor recommending controls that are not applicable to the organization. This, in turn, can damage your reputation with the auditee and, ultimately, with senior management.

Figure 1—Existing Audit/Assurance Programs

Source	Description
ISACA	Audit/assurance programs[4]
IIA	Global Technology Audit Guides (GTAGs)[5]
AuditNet	Audit Programs[6]

Source: Ian Cooke. Reprinted with permission.

Build Your Own

During your career as an IS auditor, there will be a requirement to build your own audit/assurance programs. These would typically be required when the audit subject is a custom-built application or when the organization being audited is implementing tools or processes that are on the cutting edge. How do you approach such assignments?

In March 2016, ISACA released an excellent white paper titled *Information Systems Auditing: Tools and Techniques Creating Audit Programs*.[7] The paper describes the five steps in developing your own audit program (**figure 2**). Essentially, these steps are:

1. **Determine audit subject**—What are you auditing? This is often set as part of the overall audit plan.
2. **Define audit objective**—Why are you auditing it? Again, this may have been set as part of the overall audit plan.
3. **Set audit scope**—What are the limits to your audit?
4. **Perform preaudit planning**—What are the specific risk factors?
5. **Determine audit procedures and steps for data gathering**—How will you test the controls for these risk?

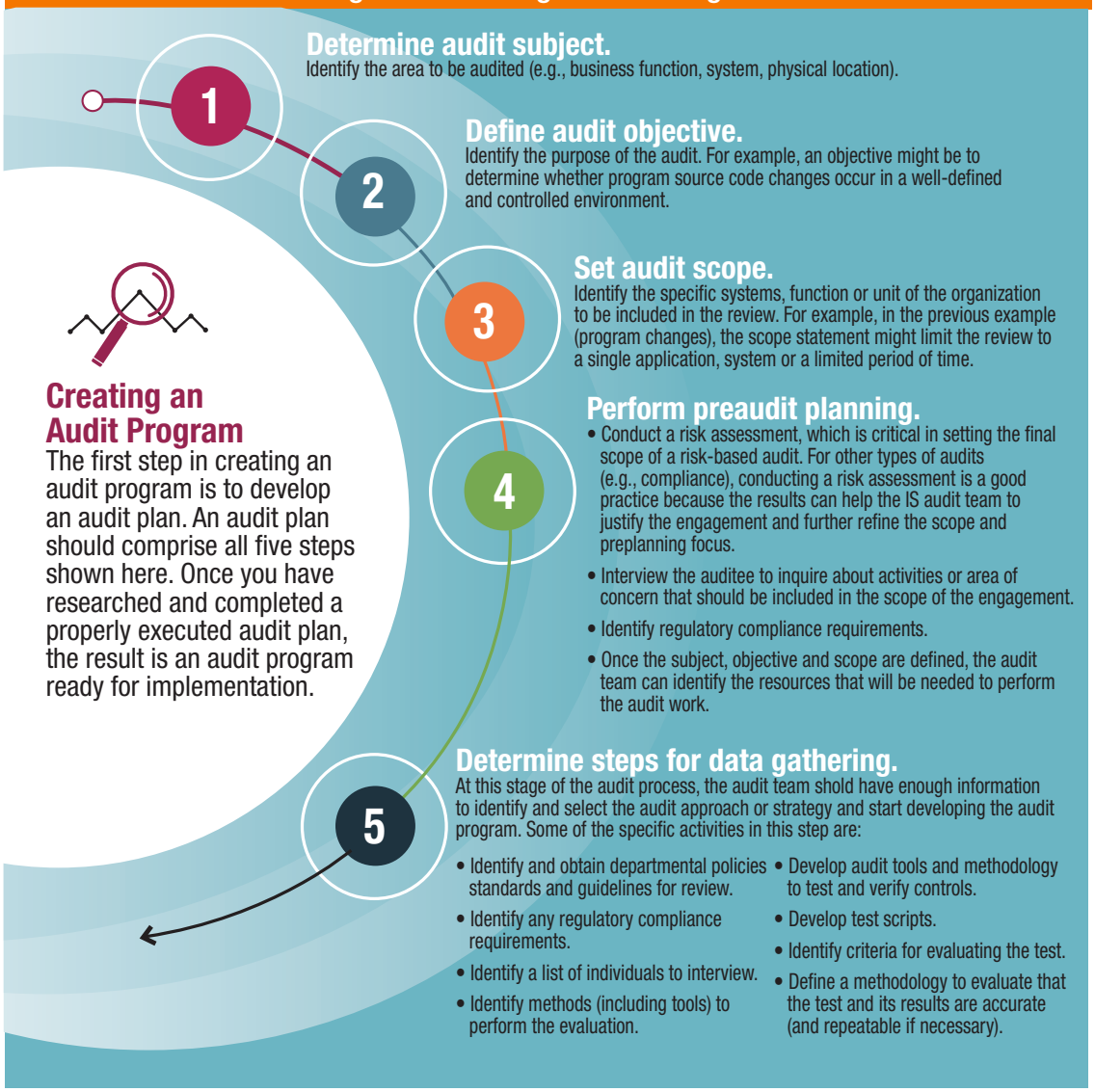
A crucial component of step 5 is developing the criteria for evaluating tests. “Criteria” is defined as the standards and benchmarks used to measure

Ian Cooke, CISA, CRISC, CGEIT, COBIT Assessor and Implementer, CFE, CPTE, DipFM, 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 current member of ISACA’s CGEIT® Exam Item Development Working Group. He is the community leader for the Oracle Databases, SQL Server Databases, and Audit Tools and Techniques discussions in the ISACA Knowledge Center. Cooke assisted in the updates of the *CISA® Review Manual* for the 2016 job practices and was a subject matter expert for ISACA’s CISA Online Review Course. 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 at Ian_J_Cooke@hotmail.com, Twitter (@COOKEI) or on the Audit Tools and Techniques topic in the ISACA Knowledge Center. Opinions expressed in this column are his own and do not necessarily represent the views of An Post.

and present the subject matter and against which an IS auditor evaluates the subject matter.[8] Many of these will be defined by the entity that is being audited (e.g., contracts, service level agreements, policies, standards); however, there will be instances, for example, when an organization has not defined its own standards when other criteria should be applied (**figure 3**).

One such instance might be when you are auditing an Oracle database. Where an organization has defined its own Oracle database standard, then you audit to that standard. However, if no standard exists, it is good practice to use an external benchmark if it is objective, complete, relevant, measurable, understandable, widely recognized, authoritative and understood by, or available to, all readers and users of the report.[9] Further, IS audit

Figure 2—Creating an Audit Program



Source: ISACA®, Audit Plan Activities: Step-By-Step, 2016

Enjoying this article?

- Read ***Information Systems Auditing: Tools and Techniques—IS Audit Reporting.*** *www.isaca.org/creating-audit-programs*
- **Learn more about, discuss and collaborate on audit tools and techniques in the Knowledge Center.** *www.isaca.org/it-audit-tools-and-techniques*

Figure 3—Sources of Assurance/Good Practice	
Source	**Description**
ISACA	COBIT 5[10] White papers[11] Cloud computing guidance[12] Cyber security resources[13]
US Department of Defense	Security Technical Implementation Guides (STIGs)[14]
CIS	Center for Internet Security Benchmarks[15]
ISO	International Organization for Standardization, ISO/IEC 27000 family—*Information security management systems*[16]
CSA	Cloud Security Alliance[17]
NIST	US National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity[18] Security and Privacy Controls for Federal Information Systems and Organizations[19] NIST publications[20]
PCI DSS	Payment Card Industry Data Security Standard[21]*
ITIL	Information Technology Infrastructure Library[22]
*ISO and PCI DSS can also be used as sources of best practice even where compliance is not required.	

Source: Ian Cooke. Reprinted with permission.

and assurance professionals should consider the source of the criteria and focus on those issued by relevant authoritative bodies before accepting lesser-known criteria.[23] I would also disclose the criteria used and why—in this case, auditors were required to give an opinion on the security of an Oracle database, but management had no standard defining what "secure" means. A further finding from such an audit may be that management should define such a standard. Selecting the right criteria is vital for the success of the audit.

Collaborate

We live in a world where it is very much a viable option to run a business using open-source software. I, therefore, pose a simple question: Why cannot we, as an ISACA community, develop open-source audit/assurance programs?

The Documents and Publications section of Audit Tools and Techniques[24] allows every member to contribute user-created documents and publications. Members could, therefore (with their organization's permission), upload completed audit/assurance programs, making them available (with the right terms and conditions) for other members to adopt for their own enterprise's risk and criteria. Further, other members could contribute to and enhance these documents. Over time, we, as a community, could build up many audit/assurance programs that are continuously enhanced and kept up to date.

Conclusion

An audit/assurance program is defined by ISACA as a step-by-step set of audit procedures and instructions that should be performed to complete an audit.[25] Many of these steps are common to most enterprises; however, each also has its own culture, ethics and behavior. We can utilize and share existing audit/assurance programs and even

> **"Why cannot we, as an ISACA community, develop open-source audit/assurance programs?"**

collaborate on the building of same if we remember that we have an obligation to consider the risk to our own organizations.

Editor's Note

ISACA is currently exploring several methods for community-driven audit program sharing and development models.

Endnotes

1 ISACA® Knowledge Center, Audit Tools and Techniques, *www.isaca.org/it-audit-tools-and-techniques*
2 ISACA Knowledge Center, Oracle Databases, *www.isaca.org/topic-oracle-database*
3 ISACA Knowledge Center, SQL Server Databases, *www.isaca.org/topic-oracle-database*
4 ISACA, Audit/Assurance Programs, *www.isaca.org/auditprograms*
5 Institute of Internal Auditors, Global Technology Audit Guides, *https://na.theiia.org/standards-guidance/topics/Pages/Information-Technology.aspx*
6 AuditNet, Audit Programs, *www.auditnet.org/audit_programs*
7 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*
8 ISACA, ITAF: Information Technology Assurance Framework, USA, 2014, *www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/ObjectivesScopeandAuthorityofITAudit.aspx*
9 *Op cit*, ITAF, p. 20
10 ISACA COBIT 5, USA, 2012, *www.isaca.org/cobit/pages/default.aspx*
11 ISACA, White Papers, *www.isaca.org/Knowledge-Center/Research/Pages/White-Papers.aspx*
12 ISACA, Cloud Computing Guidance, *www.isaca.org/Knowledge-Center/Research/Pages/Cloud.aspx*
13 ISACA, Cyber Security Resources, *www.isaca.org/KNOWLEDGE-CENTER/RESEARCH/Pages/Cybersecurity.aspx*

14 Department of Defense, Security Technical Implementation Guides, USA, *http://iase.disa.mil/stigs/Pages/index.aspx*
15 Center for Internet Security Benchmarks and Controls, *https://benchmarks.cisecurity.org/downloads/*
16 International Organization for Standardization/International Electrotechnical Commission, ISO/IEC 27000 Family—Information Security Management Systems, *https://www.iso.org/isoiec-27001-information-security.html*
17 Cloud Security Alliance, *https://cloudsecurityalliance.org/group/security-guidance/#_downloads*
18 National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, USA, *https://www.nist.gov/cyberframework*
19 Security and Privacy Controls for Federal Information Systems and Organizations, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*
20 National Institute of Standards and Technology, NIST publications, *https://www.nist.gov/publications*
21 Payment Card Industry Data Security Standard, *https://www.pcisecuritystandards.org/*
22 Information Technology Infrastructure Library, *https://www.itil.org.uk/all.htm*
23 *Op cit*, ITAF, p. 20
24 *Op cit*, ISACA Knowledge Center
25 ISACA Glossary, *https://www.isaca.org/Pages/Glossary.aspx*