IS AUDIT BASICS

Innovation in the IT Audit Process

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/2Eqjnfz

In June 2015, ISACA® began publishing a set of white papers titled "Innovation Insights."[1] The papers covered the top 10 emerging digital technology trends most likely to deliver significant value, in excess of cost, to the vast majority of enterprises.[2] The topics covered included big data analytics, mobile, cloud, machine learning, the Internet of Things (IoT), massive open online courses, social networking, digital business models, cybersecurity and digital currency. Unfortunately, from an audit perspective, the papers were targeted at business leaders and board members. While they are not all topics that an IT auditor can influence on a day-to-day basis, does that mean that IT auditors cannot innovate?

Innovation is defined as the introduction of something new or a new idea, method or device[3]; therefore, introducing something new to a process is innovating. Further, if it is new to the enterprise, it is also innovation. So, how can we innovate throughout the IT audit process?

According to ISACA, the typical audit process consists of three phases (**figure 1**). The following are my thoughts for potential innovation during each phase. Please bear in mind that what may be new and innovative for enterprise A may be business as usual for enterprise B.

Ian Cooke, CISA, CGEIT, CRISC, 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 supported the update of the *CISA Review Manual* for the 2016 job practices and was a subject matter expert for 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), or on the Audit Tools and Techniques topic in the ISACA Knowledge Center. Opinions expressed are his own and do not necessarily represent the views of An Post.

Planning—Collaborate

The Internet allows us to communicate with peers instantly and has enabled innovative ways of doing many things. Fundamentally, however, we are each still planning and creating audit programs as if this revolution had not taken place. In an earlier column,[4] I advocated for the ISACA community to develop open-source audit/assurance programs. In the meantime, organizations can innovate by collaborating on audit/assurance programs through their local chapters or industry groups. For example, does the next seminar have to take the format of an expert explaining the fundamentals of a new law or regulation? Can it not be a facilitated open forum that results in, or at least is the basis for, an audit program for said regulation?

Also, please remember that collaboration is always possible in the ISACA Knowledge Center.[5]

Planning—Implement Audit Management Software

Over the years there have been several discussions on the ISACA Knowledge Center on the benefits (or otherwise) of adopting audit management software. Those against point to the inflexibility of many of the tools available and the fact that it is just easier to get things done with Microsoft Word and Excel. However, one of the real benefits is that they enforce a standardized process. This is the very essence of what we, as auditors, like to see in processes we review.

Standardization ensures that each audit goes through steps defined and agreed on by the enterprise. These will likely include risk assessment, peer review and audit management approval. They will, in turn, improve the quality and consistency of audits. Consistency of message is key for audit functions and, indeed, for auditees.

Further, it means that IT auditor A should be in a better position to pick up, understand and continue work initiated by IT auditor B.

Planning—Utilize Data Analytics Earlier

Traditionally, the use of data analytics is considered only at the audit fieldwork stage. However, if an engagement enables access to all the enterprise's data for the subject under review, then it may be worth employing data analytics earlier. By mining the data, it is possible to determine which countries, business units, and business processes or other areas hide outliers that could represent increased risk or compliance issues. Once a business unit or geography is identified, the scope of the engagement can be further refined by drilling deeper into the data, increasing scope in higher-risk areas and reducing scope in sectors where analytics suggests the risk may be less. The overall result is a more dynamic audit plan based on continuous, just-in-time risk assessment; more efficient audits that are aligned with areas of risk; more effective results from audits that are focused on those areas of high risk; and automated reporting.[6]

> "TRADITIONALLY, THE USE OF DATA ANALYTICS IS CONSIDERED ONLY AT THE AUDIT FIELDWORK STAGE."

Planning—Implement Control Self-Assessment

In enterprises where a sizable portion of the evidence is provided by interviewing and there is a good, proven working relationship between

management and audit, one can truly innovate and save significantly on time by adopting control self-assessment (CSA). CSA was also discussed in a previous column.[7] To recap, ISACA defines CSA as an assessment of controls made by the staff of the unit or units involved. It is a management technique that assures stakeholders, customers and other parties that the internal control system of the organization is reliable.[8]

CSA requires the auditee to answer a series of questions on the relevant criteria or the standards and benchmarks used to measure and present the subject matter and against which an IS auditor evaluates the subject matter.[9] With management agreement, these results can be used as a basis for audit recommendations.

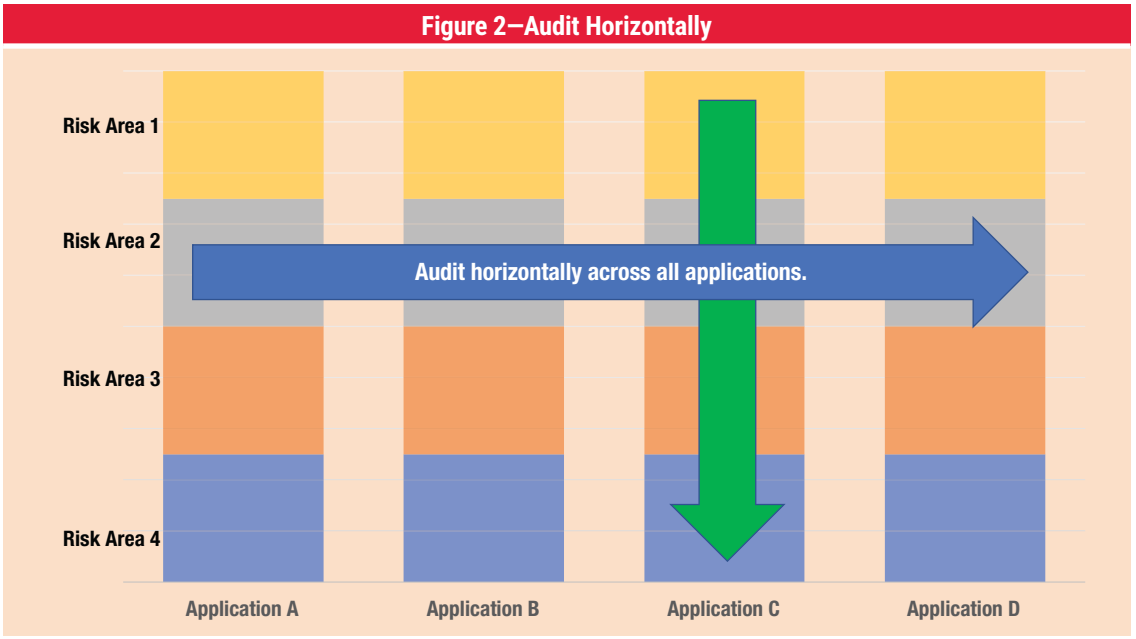
Planning—Audit Horizontally

It is widespread practice to audit applications or subject areas horizontally, that is, reviewing all the

Figure 1—Typical Audit Process Phases

Source: ISACA, *Information Systems Auditing: Tools and Techniques—Creating Audit Programs*, USA, 2016. Reprinted with permission.

Figure 2—Audit Horizontally



selected risk areas for a given application. Each application or subject is audited independently (**figure 2**). However, auditing in this manner can result in recurring findings or common themes.

> "IF THE IT AUDITOR IS GIVEN PRIMARY, READ-ONLY ACCESS TO THIS EVIDENCE, IT WILL REDUCE THE TIME THE AUDITOR NEEDS TO SPEND WITH THE AUDITEE, ULTIMATELY SAVING THE ENTERPRISE MONEY."

For example, several applications may not be fully compliant with the defined change management process. This will result in multiple similar findings across the different applications. In such circumstances, it may make sense to audit the change management process itself horizontally across all the applications (**figure 2**) perhaps utilizing the COBIT® 5 enablers.[10] The purpose of such an audit would be to address the underlying causes of the recurring theme and mitigate risk across several applications.

Fieldwork/Documentation—Get Primary Access to the Evidence

At the fieldwork stage of an audit, an IT auditor attains evidence to measure against the criteria. The traditional way to do this is via interviewing and walk-throughs, where the IT auditor will ask for a print screen, copy of a report or other evidence to confirm that the criteria have been met. However, if the IT auditor is given primary, read-only access to this evidence, it will reduce the time the auditor needs to spend with the auditee, ultimately saving the enterprise money.

Further, the IT auditor need not be limited to sampling. Some examples follow:

- **Change management**—If a change management application is in place and the IT auditors have direct access to it, they do not necessarily need to walk through the changes with the auditee. They can sample or test all changes directly on the application or by extracting the data from the application for further analysis.
- **Vulnerability management**—If the IT auditors have direct, read-only access to the vulnerability scanner, they can tell if the associated assets are being scanned by the tool. Further, by reviewing the results of previous scans they can gain assurance on whether an ongoing process is in place and vulnerabilities are continuously being mitigated.

- **Audit and logging**—If the IT auditors have direct, read-only access to the enterprise's security information and event management (SIEM) tool, they can tell whether the related application assets are captured in the tool and the auditing is at a level that matches the required criteria.

This concept could also be applied to other processes where automated software is in use or evidence is captured and maintained by second-line functions.[11] This could include the leavers and movers process, disaster recovery testing, backup restore testing, and database scanners.

Fieldwork/Documentation—Repurpose Generalized Audit Software

ISACA defines generalized audit software (GAS) as multipurpose audit software that can be used for general processes, such as record selection, matching, recalculation and reporting.[12] From an IT auditor's perspective, the use of GAS tools is traditionally restricted to supporting operational or general audits by aiding in the extraction and analysis of data from the database of a given application. However, these tools will equally support data extracted from servers, application logs and views, and meta data from databases. They can be used, therefore, to support IT audits.

Once extracted, the data can be analyzed and compared against known compliant data sets and other sources of data, such as the company payroll. Further, the process can be repeated and used as part of a continuous monitoring and/or audit. Examples of this approach in use include "Auditing Oracle Databases Using CAATs"[13] and "Auditing SQL Server Databases Using CAATs."[14]

Reporting/Follow-Up—Utilize the ISACA Glossary

In a 2015 white paper, ISACA defined the five attributes of an audit finding (**figure 3**).[15] A potential issue with the condition attribute is that the report audience may not always be technical even though a technical finding is being described. Therefore, it makes sense to include a definition of the area under review with the audit finding (e.g., vulnerability management). An effective way to do this is to use the definitions from the ISACA glossary.[16] This provides clear explanations and will also create consistency, in that vulnerability management, for example, will be defined in the same way across multiple audit reports. This, in turn, means that the audience will learn and understand the terminology over time.

Even, if the ISACA glossary does not currently meet organizational needs, it can be used as a baseline or starting point.

Reporting/Follow-Up—Use Video

IT audit reports can be complex documents containing layers of interrelated findings that affect multiple areas of the business and often require further explanation. This may be overcome by

Figure 3—Attributes of an Audit Finding

Attribute	Description	Identifies
Condition	Findings	Identifies the auditor findings. It is a statement of the problem or deficiency. This may be in terms such as control weaknesses, operational problems, or noncompliance with management or legal requirements.
Criteria	Requirements and baseline	Statement of requirements and identification of the baseline that was used for comparison against the auditor findings, based on the audit evidence.
Cause	Reason for the condition	While the explanation of the cause may require the identification of the responsible party, it is suggested that, unless required by audit policy, the report should identify the organizational business unit or person's title and not the individual's name. The same should be applied to the identification of the person representing the relevant point of accountability.
Effect	Impact of the condition	The statement of impact answers the question "So what?" It explains the adverse impact to the operational or control objective. By articulating impact and risk, the element of effect is very important in helping to persuade auditee management to take corrective action.
Recommendation	Suggested corrective action	While the corrective action should eliminate the problem or deficiency noted in the condition, the corrective action should be directed toward addressing the cause.

Source: ISACA, *Information Systems Auditing: Tools and Techniques—IS Audit Reporting*, USA, 2015. Reprinted with permission.

Enjoying this article?

- Learn more about, discuss and collaborate on IT audit tools and techniques in the Knowledge Center. *www.isaca.org/it-audit-tools-and-techniques*

meeting the audience face-to-face and providing further detail. However, due to the size, complexity and geographical dispersity of some enterprises, this is not always possible.

I had the honor of working with a colleague on an ISACA committee who overcame this problem by recording the executive summaries on video. The videos were uploaded to a private YouTube channel with the required technical controls (e.g., two-factor authentication). Besides adding context and meaning to the audit reports, it also allowed him to deliver the results with empathy—something that is difficult to get across in a written report.

Reporting/Follow-Up—Track and Measure Progress

ISACA's Information Technology Assurance Framework (ITAF) recommends that a report on the status of agreed-upon corrective actions arising from audit engagement reports, including agreed-upon recommendations not implemented, should be presented to the appropriate level of management and to those charged with governance (e.g., the audit committee).[17] This can be achieved by bringing the recommendations together in an assurance-finding register.

In addition, if these findings are allocated attributes (e.g., significance, status, owner, country, department, region), the data can be analyzed, summarized and presented in a meaningful manner—becoming information. This information can then be used to clearly show compliance to standards and regulations and even act as lead indicators for new initiatives. For further details, see "Enhancing the Audit Follow-up Process Using COBIT 5."[18]

Conclusion

My overall message is that innovation, much like beauty, is in the eye of the beholder. If it is new to the enterprise, it is innovation. Furthermore, innovation does not have to include the latest technology, such as machine learning. Neither does it have to be a revolution; it can be an evolution. To innovate, we auditors do not have to be futurists; we can be "now-ists."[19]

> "INNOVATION, MUCH LIKE BEAUTY, IS IN THE EYE OF THE BEHOLDER."

Endnotes

1 ISACA, "Innovation Insights," USA, 2015, *www.isaca.org/Knowledge-Center/Research/Pages/isaca-innovation-insights.aspx*
2 *Ibid*.
3 Merriam-Webster, "Innovation," *https://www.merriam-webster.com/dictionary/innovation*
4 Cooke, I.; "Audit Programs," *ISACA® Journal,* vol. 4, 2017, *https://www.isaca.org/archives/*
5 ISACA Knowledge Center, Audit Tools and Techniques, *www.isaca.org/Groups/Professional-English/it-audit-tools-and-techniques/Pages/Overview.aspx*
6 Kress, R.; D. Hildebrand; "How Analytics Will Transform Internal Audit," *ISACA Journal,* vol. 2, 2017, *https://www.isaca.org/Journal/archives/Pages/default.aspx*
7 Cooke, I.; "Doing More with Less," *ISACA Journal*, vol. 5, 2017, *https://www.isaca.org/archives/*
8 ISACA, *CISA Review Manual, 26th Edition*, USA, 2016
9 ISACA, ITAF: Information Technology Assurance Framework, USA, 2014, *www.isaca.org/Knowledge-Center/ITAF-IS-Assurance-Audit-/IS-Audit-and-Assurance/Pages/ObjectivesScopeandAuthorityofITAudit.aspx*
10 ISACA, COBIT® 5, USA, 2012, *www.isaca.org/COBIT/Pages/default.aspx*

11 Chartered Institute of Internal Auditors, "Governance of Risk: Three Lines of Defence," *https://www.iia.org.uk/resources/audit-committees/governance-of-risk-three-lines-of-defence/*

12 ISACA Glossary, *https://www.isaca.org/glossary*

13 Cooke, I.; "Auditing Oracle Databases Using CAATs," *ISACA Journal,* vol. 2, 2014, *https://www.isaca.org/archives/*

14 Cooke, I.; "Auditing SQL Server Databases Using CAATs," *ISACA Journal*, vol. 1, 2015, *https://www.isaca.org/archives/*

15 ISACA, *Information Systems Auditing: Tools and Techniques—IS Audit Reporting*, USA, 2015, *www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/information-systems-auditing-tools-and-techniques.aspx*

16 *Op cit* ISACA Glossary

17 ISACA, *ITAF™: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition*, USA, 2014, *www.isaca.org/ITAF*

18 Cooke, I.; "Enhancing the Audit Follow-Up Process Using COBIT 5," *ISACA Journal,* vol. 6, 2016, *https://www.isaca.org/archives/*

19 Ito, J.; "Want to Innovate? Become a 'Now-ist,'" TED, 2014, *https://www.ted.com/talks/joi_ito_want_to_innovate_become_a_now_ist*