IS audit basics

Risk-based Audit Planning for Beginners

A young Certified Information Systems Auditor® (CISA®) asked for suggestions about where and how to start to plan an IS audit. As the question was not more specific than that, the reply was, "It all depends," and a few questions had to be asked to better understand the context. There was agreement from the outset that the traditional general controls review would not be the best approach.

This column presents the questions that would provide enough information to get started and the subsequent steps to come up with a realistic audit plan that adds value to the organization.

Basic Information Needs

If the auditor is a member of an internal audit organization, a good deal of information should be readily available and there will be colleagues able to share it and put it in context. This must include the definition of any applicable regulatory framework as well as any preferred audit standards (e.g., COBIT®). If the audit is to be outsourced to an external entity, gathering the remaining information may prove more laborious.

Q1: Why has the audit been proposed or requested?
Requesting an information systems (IS) audit is, in itself, a valuable indicator. There are three reasons for doing this:

1. An outgoing (retirement, change of job) chief information officer (CIO) wishes to prepare an independent assessment for his/her successor—a commendable practice that also protects the individual from blame or criticism after his/her departure.
2. The senior management of the organization has concerns about the performance of the IS function and wishes to understand what the root causes are and how to address them.
3. The audit committee requests it because the IS audit history is considered unsatisfactory.

> **"The size and complexity of an organization defines its dependence on and the criticality of its information systems and services and, therefore, its audit needs."**

Q2: Describe the organization and its IS/IT.
The size and complexity of an organization defines its dependence on and the criticality of its information systems and services and, therefore, its audit needs. It is reasonable to assume that large organizations where IS/IT plays a critical role, such as e-commerce, utilities and law enforcement, have internal audit strategies, competent audit committees and external auditors to guide them as appropriate. Young auditors can expect to develop and grow in such an environment. If this is not the case, they should consider continuing their career elsewhere.

Ed Gelbstein, Ph.D., 1940-2015
Worked in IS/IT in the private and public sectors in various countries for more than 50 years. Gelbstein did analog and digital development in the 1960s, incorporated digital computers in the control systems for continuous process in the late '60s and early '70s, and managed projects of increasing size and complexity until the early 1990s. In the '90s, he became an executive at the preprivatized British Railways and then the United Nations global computing and data communications provider. Following his (semi)retirement from the UN, he joined the audit teams of the UN Board of Auditors and the French National Audit Office. Thanks to his generous spirit and prolific writing, his column will continue to be published in the *ISACA® Journal* posthumously.

Small organizations constitute a special case: They will not have the resources to properly apply good practices (e.g., IT Infrastructure Library [ITIL][1] and Data Management Body of Knowledge [DMBOK][2]), frameworks such as COBIT® 5,[3] or standards such as International Organization for Standardizations (ISO) ISO 20000 (service management) or ISO 27000 (security). A previous column[4] in this series addressed the special case of auditing small IT organizations.

Q3: What is the audit history?
Knowing what audits took place in the last X (perhaps three to five) years and what their outcomes were should provide good insights into the strengths and weaknesses of IS/IT. Signs to watch for include:

- Infrequent general controls reviews, i.e., a questionnaire-based, box-ticking exercise that covers the essentials, but has little or no relation to the business risk associated with information systems and data
- Recommendations from past audits that were not implemented. The statement "things have changed," often given as a reason, should not be taken at face value.

Q4: What about metrics, performance and risk indicators?
Good management and the higher levels of maturity require reliable measurements for the CIO and business managers, the latter expressed in terms meaningful to nontechnical people (e.g., the cost of downtime or number of records compromised).

Lagging indicators are useful to determine trends (improvement or deterioration), but cannot be relied upon for predictions of future performance, which need leading indicators. COBIT 5 provides extensive descriptions of both lagging and leading indicators for each process it covers.

Q5: Describe the enterprise's risk assessment and management program.
Risk-based auditing developed more than a decade ago to support corporate governance. It is considered to deliver greater value than a traditional audit or general controls review and requires a sound understanding of the business, its objectives and risk, and, therefore, the adequacy of its controls.

As risk-based auditing combines business knowledge, risk assessment and strategic audit before deploying audit resources, it allows the internal audit function to focus on risk domains proportionate to the business's potential exposures.

A properly conducted risk assessment would, ideally, be based on a recognized framework such as *COBIT® 5 for Risk* (there are other frameworks such as one from the US National Institute of Standards and Technology [NIST][5] and Operationally Critical Threat, Asset, and Vulnerability Evaluation [OCTAVE][6]) and include a ranked register that can be used to identify which risk factors are dependent on information systems and services.

Findings

The answers to the five questions should provide a robust understanding of the starting point for the proposed audit. They may also raise additional questions. The absence of past audits, implemented recommendations, metrics and risk assessments are themselves important findings that should set the tone for the proposed audit.

Mapping the Information Collected Against the IS Audit Universe

The IS audit universe is undergoing a relentless expansion that, in turn, needs updated and new policies, practices, frameworks and audit guidelines. A high-level view of the current audit universe would include:

- **Governance**—IS/IT strategy, policies, sourcing decisions, human resources, findings, performance monitoring and audits
- **Operations 1**—Data centers, local and wide area networks, physical and logical security, disaster recovery and business continuity, local networks, and Internet access by branch offices away from headquarters. COBIT 5 and ITIL cover this topic admirably.
- **Operations 2**—Systems and technologies not managed by the IS/IT function, typically industrial automation and supervisory control and data acquisition (SCADA) systems

- **External service providers**—Telecommunications, outsourcers, cloud service providers, maintenance companies, consultants, auditors, contract and relationship management, performance monitoring, and management (both at headquarters and delegated to remote offices)
- **Business applications**—Software (both packaged and custom), mobile apps, end-user computing (particularly spreadsheets and personal databases), license management, updates, patches and fixes, change management, accreditation, etc.
- **Mobile**—Bring your own device (BYOD), lost and compromised devices, access to sensitive corporate data, participation in social networks, disclosures of sensitive information, etc.
- **Security**—Frameworks (e.g., ISO 27001 or NIST SP800), awareness, certifications, breaches, etc.
- **Risk management**—Frameworks (e.g., *COBIT 5 for Risk*), risk assessments, mitigation measures, reviews, etc.
- **Data**—Quality, classification, data models, database administration, etc., and guidelines used (e.g., DMBOK)
- **IS/IT projects**—Departures from plan (time/budget), change management, project management, changing risk areas, etc.

To this list one could add human factor issues such as ability to exploit systems and technologies, training and continuing education, and many more things that will be defined by the nature of the business.

The information gathered from the responses to the previous section's five questions should be analyzed and mapped against this list, which outlines the audit universe. This will help identify areas of greatest risk, gaps in coverage and IS/IT's contribution.

Formulating a Draft Audit Plan

It is not sensible to believe that a small group of auditors (or even a large group) can do justice to all the items in the preceding list, and this means choices have to be made as to what gets audited and when. The mapping exercise in the previous section should deliver the information required to correlate the most important areas of business risk against the role that IS/IT plays in each of them.

Once IS/IT's role has been identified, it is up to the auditors, in discussion with risk managers and the CIO, to specify the scope and granularity of the audit, i.e., what merits auditing, the controls to be assessed and the rationale for doing so.

> **"The IS audit universe is undergoing a relentless expansion that, in turn, needs updated and new policies, practices, frameworks and audit guidelines."**

Some of these risk areas may have no IS/IT direct component. For example, nongovernmental organizations providing humanitarian support (famine, medical, refugee assistance, war relief) in unstable regions may be more concerned with protecting their personnel from being taken hostage

than an IS service interruption. To limit this risk, their practices and controls consist of not providing data about them online and advising them not to disclose information on social networks.

Discussing the Draft Plan

It is at this stage that it becomes possible to decide whether such an audit would be a sensible use of resources (of both audit and audit clients). This should be addressed first with the chief audit executive and then with the audit clients. If agreement to proceed is reached, the next steps are to explore who will conduct the audit, when, who will need to be involved and how long it will take to complete the process.

Endnotes

1 Information Technology Infrastructure Library, *www.itil.org.uk*

2 Data Management Association International, Data Management Body of Knowledge, *www.dama.org*

3 ISACA®, COBIT® 5, USA, 2012, *www.isaca.org/COBIT/Pages/default.aspx*

4 Gelbstein, E., "Auditing Small IS/IT Organizations," *ISACA® Journal*, vol. 4, 2015, *www.isaca.org/Journal/archives/*

5 National Institute of Standards and Technology, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST SP 800-37, USA, 2014, *http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf*

6 Carnegie Mellon University, Software Engineering Institute, Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) methodology, Pittsburgh, Pennsylvania, USA, *www.cert.org/resilience/products-services/octave/*