IS audit basics

Elements of an IS/IT Audit Strategy, Part 2

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.

Part 1 of this series concluded at the end of the cycle shown in **figure 1** (included in part 1 as well), i.e., considering the audiences for the strategy (in addition to the audit function) and the minimum contents that make it viable.

This article, Part 2, discusses how the key elements of the audit universe that are included in the audit strategy and its derived audit plans are chosen to reflect business risk. It also addresses what information is required to do this, who can supply it and the role of the various participants in the process. Accountability for delivering a viable and realistic strategy remains with the chief audit executive (CAE).

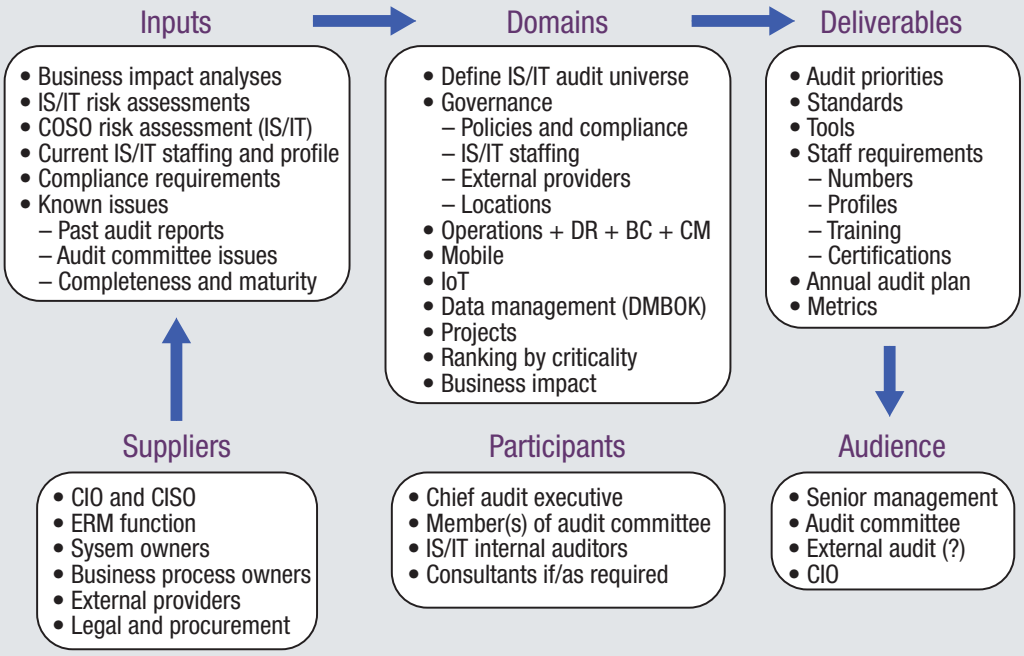
The IS/IT Universe

The contents of the domains box in **figure 1** are generic and incomplete to avoid complicating the diagram. It could also include end-user computing (e.g., undocumented spreadsheets used to support critical decisions, personal databases) and rapidly adopted technologies such as social media a few years ago and, more recently, bring your own device (BYOD). Both of these technologies have caused considerable disruption in many organizations by bypassing business and technical strategies and, in the case of BYOD, invalidating the organization's technical architecture.

Innovations of this kind can be expected to continue to be enthusiastically adopted by the workforce despite corporate policies. The managerial and audit challenges arise because their discovery is invariably after the fact, as workers illustrate the truth of the old adage that it is easier to seek forgiveness than permission.

A comprehensive, end-to-end audit of the organization's information systems and technology

Figure 1—Elements of an IS/IT Audit Strategy



IoT = Internet of Things
DMBOK = Data management body of knowledge

Source: Ed Gelbstein. Reprinted with permission.

is out of the question, as it would paralyze the IS/IT function and many elements may not be auditable for contractual reasons. However, each organization must determine which domains to audit because the activities, criticalities and impact of each domain depend on what information systems and technology do and how each element contributes to business risk.

Figure 2 gives an overview of factors that should be considered to prioritize the risk/impact elements of the IS/IT audit universe. Other factors may need to be included to reflect the nature of the organization developing the strategy.

This article assumes that neither the internal auditor nor the chief information officer (CIO) is qualified or knowledgeable enough to assess how these elements contribute to business risk. Business impact analyses may help as long as they are constantly reviewed and updated (not always likely) and have a clear business owner.

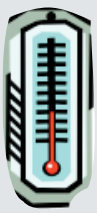
Therefore, the issue becomes identifying who can perform the following functions:

- Map technology risk to business risk.
- Assess technology risk (ideally, quantitatively) integrated with the other risk domains that are part of enterprise risk management (ERM)
- Rank all areas of risk so that the auditors can focus on how the IS/IT function addresses risk and works toward separating the critical few from the trivial many.

At this point, several members of the organization must supply critical information as an input to the process of identifying and prioritizing business risk areas driven by IS/IT, which will ultimately be reflected in the audit strategy and related audit plans. These suppliers would normally include, at a minimum:

- The CIO and the chief information security officer (CISO), or equivalent titles. While these positions have a primarily technical responsibility and act as custodians of the corporate information (and data) as well as their processing systems and databases, they are also accountable for a range of support services that can play important roles.

Figure 2—Decision Factors in Support of an IS/IT Audit Strategy



Criticality of IT

L, M, H, Extreme

IT Organization

- Size
- Governance
- Performance
- Business unit autonomy
- End-user apps
- Outsourcing/offshoring

Small IT organizations are a special case.

Risk Domains

- Financial
- Compliance
- Operational
- Reputational

Size of IT Activity

S, M, L, XL, XXL

Known issues

- Performance
- Technical
- People
- Service providers
- IT audit resources
- Audit/consultancy balance

IT Audit History

- Date of last audit
- Recommendations
- Follow-up actions

Source: Ed Gelbstein. Reprinted with permission.

Those services include Internet access, email, support of mobile technologies, and disaster recovery and other similar plans. These individuals are accountable for identifying, assessing and mitigating threats and vulnerabilities that can impact the business and reporting them to the ERM function and others as appropriate.

- The ERM function is accountable for integrating all identified risk areas and ranking them by impact and probability of occurrence. Models like COSO's *Enterprise Risk Management—Integrated Framework* are often use for this purpose. One of the challenges to overcome arises from the difficulty in assigning probability values to IS/IT risk, partly because many threats are unknown and unknowable until they manifest themselves and partly because numerical analysis techniques are unfamiliar to many IS/IT practitioners.
- System owners are outside the IS/IT function and are accountable for the specification of the functionality of individual systems, mapping them against business processes and identifying their criticality (typically in a business impact analysis), and defining the disaster recovery and business continuity arrangements associated with each business system and, where appropriate, service.
- Business process owners are not directly concerned with individual systems, but are immediately affected by their malfunction or failure. Their most important roles are to define the business impact of such events and define the priorities for their recovery and continuity.
- External providers increasingly play a critical role in the provision of IS/IT operations. This group includes the traditional outsourced service providers, Internet and mobile access service providers, the many variants of cloud service providers (e.g., public, private, platform as a service), and external maintenance services companies. The audit strategy needs to reflect the terms of contract associated with these external parties because many exclude the possibility of being audited and others put stringent conditions on the ways and means of conducting such an audit.
- Legal counsel and the procurement function are accountable for ensuring that contracts with third parties include appropriate "right to audit" clauses and making these known to the internal audit function and other responsible parties.

The Participants in the Analysis Process

Given the size and complexity of the input to the assessment process, it would be reasonable to expect the CAE to be involved in the initiative with assistance from, typically, one or more members of the audit committee who are knowledgeable about the role of IS/IT in the organization and one or more IS/IT auditors and independent experts as and when required. In addition, it should always be possible to request the assistance of the various parties who supplied the initial information, as described in the previous section.

The output of this analysis process should drive the development of the audit strategy, as discussed in part 1 of this article.

Conclusions

Creating an IS/IT audit strategy is neither simple nor quick. Needed information may not be readily available or up to date, and the people who should be involved may find it difficult to devote sufficient time to the initiative.

On the other hand, organizations that fail to develop an audit strategy that reflects all of these factors face a real possibility of missing risk areas that could significantly—perhaps irreparably—impact their success.