IS audit basics

Elements of an IS/IT Audit Strategy, Part 1

The word “strategy” often means different things to different people. For this column, it would be pertinent to remember the story of the person who decides to walk the hills to reach a specific village without a global positioning system (GPS) device. He gets lost, but can still see the village in the distance. Encountering a shepherd, he asks the question, “How do I get to the village?” “Well,” the shepherd replies, “I would not start from here.”

This article regards an IS/IT strategy as the set of steps that will allow the chief audit executive (CAE) and the IS/IT auditors to define their starting point, identify their target state, and determine the processes and resources that will get them there. **Figure 1** provides an overview.

While the figure illustrates the sequence of events as they need to happen in practice, this discussion shall follow the reverse path, starting with the audience. The reasons for this are that senior management and the audit committee define—separately and independently—whether or not the audit strategy is approved and endorsed. They also approve the resources necessary to implement it. The opinion and agreement of the chief information officer (CIO)—the target auditee—would help in the implementation of the strategy, but if this is not forthcoming, it would be desirable to understand exactly why not. The role of the external auditors may or may not be relevant, depending on the nature of the organization and the exact role of these auditors.

Without appropriate approvals, the proposed strategy is no more than a wish list.

The IS/IT Audit Strategy Deliverables

The CAE proposing a strategy is undoubtedly aware that IS/IT is only a part, however important, of the overall audit universe of the organization. Therefore, the proposed strategy should reflect how information systems, technologies and data management fit in with the overall risk-based approach to auditing.

In April 2016, Ed Gelbstein was awarded the Michael Cangemi Best Article Award posthumously. The award recognizes individuals for major contributions in the field of IS audit, control and/or security publishing. ISACA congratulates Dr. Gelbstein’s dear wife, Cora, who received the award on behalf of her husband.

Audit Priorities

These vary from organization to organization, depending on the organization’s placement in the private or public sector, its listing in the stock exchange or private ownership, and the regulatory compliance framework in which it operates. Compliance with internal rules and regulations are also factors.

Other considerations include:

- Business activities and processes (operational, financial, legal, reputational, etc.) that have a potentially critical impact on the business
- The role of IS/IT in supporting them, indicating which have been recently audited
- Recommendations that have not been implemented and those that have been implemented, but may require being audited again

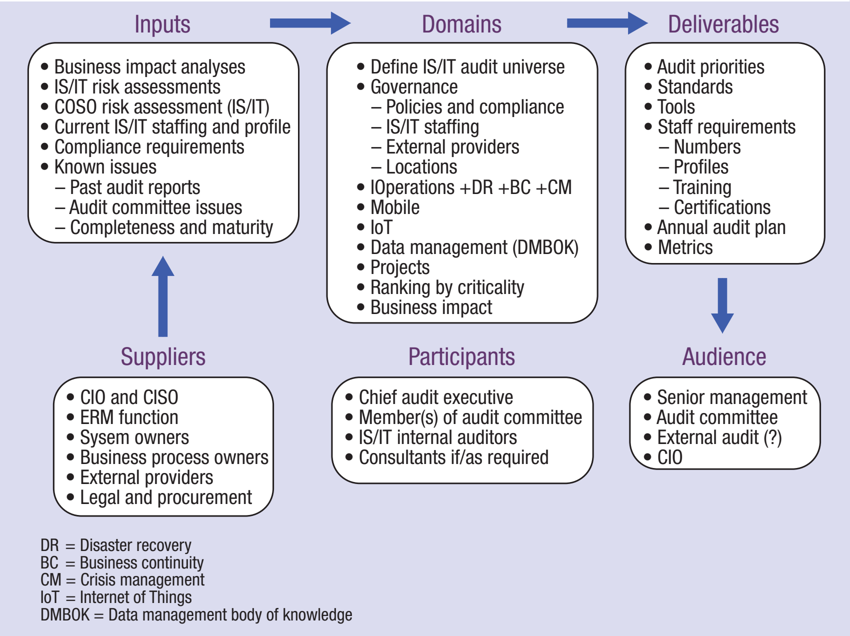
Ed Gelbstein, Ph.D., 1940-2015

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.

Do you have something to say about this article?

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

Figure 1—Elements of an IS/IT Audit Strategy



Source: Ed Gelbstein. Reprinted with permission.

Audit Standards, Frameworks and Guidelines

Relevant audits standards frameworks and guidelines are updated or revised from time to time and the CAE should ensure the latest version is adopted and indicate any transition steps required to move from the previous version to the new version. For example, the Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Enterprise Risk Management—Integrated Framework* was revised in May 2013 and, similarly, COBIT® 5 and its related documents have replaced COBIT® 4.1, Risk IT and Val IT. Transitioning from one version to the most recent is not a trivial task; it demands considerable effort and learning.

Internal auditors frequently consider the Institute of Internal Auditors (IIA) as the source of *de jure* standards and differentiate them from those used for IT and security. IS/IT auditors have several options to adopt; *de facto* standards, frameworks and guidelines are available from several sources, such as ISACA®[1] and the US National Institute of Standards and Technology (NIST). The strategy should indicate how these guidance documents complement each other and, in particular, how the proposed selection maps against the enterprise risk management (ERM) framework adopted by the business.

Tools

In particular, computer assisted audit tools and techniques (CAATTs),[2] are becoming increasingly popular, in particular those that support several functions such as:

- Continuous monitoring/continuous auditing to enable auditors to monitor user activity, applications controls and business transactions
- Data analysis and tests
- Management of working papers (essentially a centralized database of past and current audit documents). Some may debate whether this is a CAATT. Products are also available to support the standardization of formats, thus increasing the consistency (and potentially the quality) of audit documentation.

Many commercially available products exist, but they are not addressed in this article.

As in the case of standards and frameworks, (often costly) tools need to be purchased, but they are of little value unless their users are well versed in their functionality and exploit these features during the execution of the audits. This implies a commitment to learning on the part of the IS/IT auditors and an effective approach to training.

Staff Requirements

This would seem to be a simple issue to address (in theory). The IS/IT auditor is the right individual, but he/she must be knowledgeable, qualified and experienced, and have the right soft skills.[3] The challenges for the CAE and the lead IS/IT auditor are to identify and justify a strategy that covers:

- **Auditor numbers**—This requires analyzing the strategy and the associated audit plans to determine the number of auditors needed to do the work to the required degree of quality across the critical part of the business. This calls for serious considerations. Many businesses that are too small to have an ERM function or an internal auditor depend on external intervention from their headquarters if they are part of a large business (for example, the country office of a multinational located elsewhere), auditors contracted by a qualified vendor company, or an independent traveling auditor. Other businesses and the not-for-profit sector may be unable to fund a suitably resourced audit function. Outsourcing this activity is seen as being more cost-effective than recruiting and training a team.
- **Auditor profiles**—This part of the strategy must consider several characteristics of the available auditors without infringing on their right to privacy. For example, it may be pertinent to evaluate the ages of the auditors for the purpose of thinking ahead about their probable retirement time frame or their ability to move to another job elsewhere (staff turnover is a good risk indicator). Age may also indicate their experience, which may be especially relevant to certain audits. This evaluation can support the strategy in defining the role of certifications and identifying any gaps between current knowledge and that required to apply changing frameworks and guidelines. The gap analysis should also include how to bridge the gaps (formal onsite training, face-to-face courses, self-paced computer-based training or on-the-job training).
- **Annual audit plan**—This deliverable states what will be audited in the next year with enough details on timing and resources to allow the target auditee to prepare.
- **Metrics**—For the strategy to be meaningful to those who must approve it and make the resources available to implement it, the measures of success[4] that will be used to evaluate the strategy must be described, highlighting the quantifiable metrics that will be used and reported.

Conclusions

This article, which is the first of a two-part series, concentrates on what an audit strategy should deliver and to whom. This is the easy part. The challenges discussed in part 2 are in defining the continually changing and expanding IS/IT audit universe and ensuring that the focus remains on what is critical so that the audit is truly risk based.

Perhaps the hardest part is getting the full cooperation of those expected to supply information (represented by Inputs and Suppliers in **figure 1**). Few are likely to make the time to focus on this and there may be elements of organizational politics to overcome.

Endnotes

[1] ISACA, "Standards, Guidelines, Tools and Techniques," *ISACA® Journal*, vol. 3, 2016, *www.isaca.org/archives*

[2] ISACA, Audit Tools and Techniques, *www.isaca.org/Groups/Professional-English/it-audit-tools-and-techniques/Pages/Overview.aspx*

[3] Gelbstein, E.; "The Soft Skill Challenge," *ISACA Journal*, vol. 3, 2015, *www.isaca.org/archives.* Gelbstein, E.; "Is There Such a Thing as a Bad Auditor, Part 1 and 2," *ISACA Journal*, vol. 1, 2016, *www.isaca.org/archives*

[4] Gelbstein, E.; "Trust, but Verify," *ISACA® Journal*, vol 1, 2016, *www.isaca.org/journal/archives*