Auditing IS/IT Risk Management, Part 2

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.

Part 1 of this article described the commonalities, differences and possible overlaps between the IS/IT internal auditors and the IS/IT risk management functions managed by the chief information officer (CIO). It also suggested an audit universe for IS/IT risk management and introduced the case for collaboration between internal audit and enterprise risk management (ERM). **Figure 1** from part 1 is included here as a reminder.

The discussion that follows reflects the IS/IT auditor's perspective. Every topic can be subdivided into many more sections, but the intention of this column is not to provide a detailed manual (it would be a large book), just an overview.

Risk Controls

The international standard ISO 31000: 2009, *Risk management—Principles and guidelines*,[1] defines a control as "any measure or action that modifies risk. Controls include any policy, procedure, practice, process, technology, technique, method or device that modifies or manages risk."

An audit of IS/IT risk management could cover policies and procedures such as:

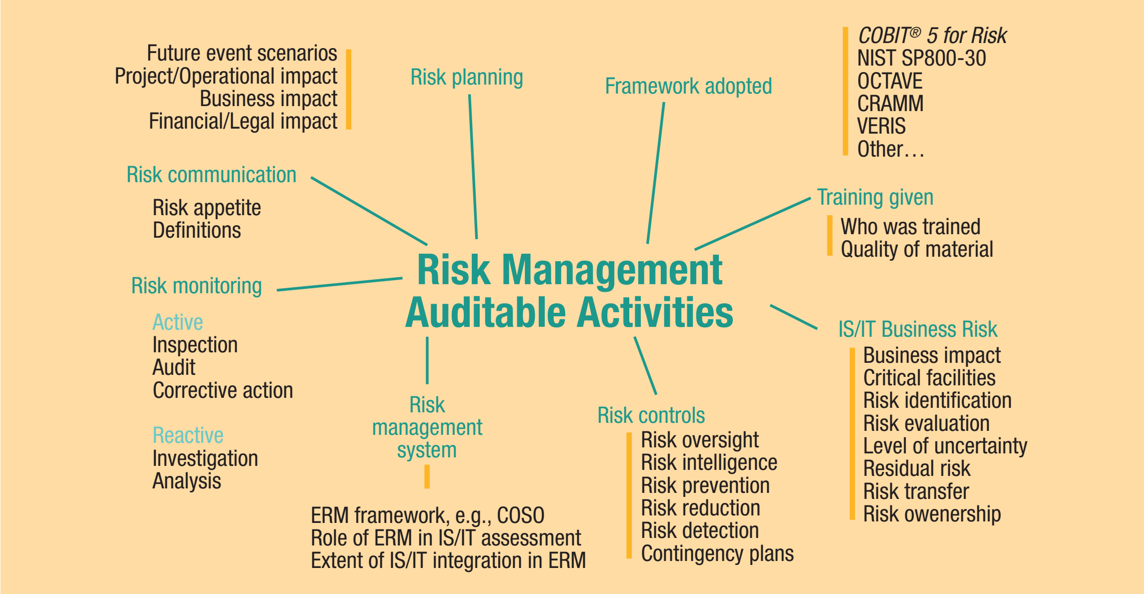
- **Risk oversight**—Audit committees and boards of management are ultimately accountable for risk oversight and should consider which individuals, teams or committees have the expertise to oversee particular risk. The auditor should seek evidence that this has been done or is being done and make observations as appropriate. If neither the audit committee nor the board are involved in the oversight of IS/IT-driven risk, a recommendation should reflect this fact.
- **Risk intelligence**—Many executives may believe that risk management requires special technical knowledge. The book *Risk Intelligence: Learning to Manage What We Don't Know*[2] disagrees and explains how four simple rules can improve risk analysis:
  1. Recognize which risk are learnable and reduce their uncertainty by discovering more about them.
  2. Identify risk you can learn about the fastest, particularly project risk.
  3. Take on risky projects one at a time. Learn about the risk underlying each before moving to the next.
  4. Build networks of business partners, suppliers and customers who can collectively manage new ventures' risk by playing distinct roles.

> **"The auditor should seek evidence that the appropriate activities are being done, to what extent and how well."**

In the specific case of IS/IT risk, risk intelligence should also include operational risk by establishing links with computer emergency response teams (CERT) and following media reports of current threats, e.g., botnets, malware, denial-of-service (DoS) attacks and industrial (and other) espionage. This sort of information does not mean the organization is no longer a target, but it does make the organization an "informed target."

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.

Figure 1—Scope of Auditable IS/IT Risk Management Activities



Source: Ed Gelbstein. Reprinted with permission.

As always, the auditor should seek evidence that the appropriate activities are being done, to what extent and how well.

- **Risk prevention**—In the same way logic indicates that a house should not be built in a flood plain, there are many IS/IT risk that can be prevented through well-established principles such as need to know, least privilege and segregation of duties (SoD). These principles need no further discussion here except to say that there are many opportunities to strengthen controls around them, but this would more likely be done in an IS/IT audit rather than an IS/IT risk management audit.
- **Risk reduction**—Also referred to as risk mitigation, risk reduction is a set of activities undertaken to reduce the impact (financial, operational, reputational, etc.) of an event. Although this topic is too large to explore in detail in this article, the auditor should seek evidence that it has been addressed, for example, by assigning ownership to the risk as well as to the measures to be taken to reduce it, ideally incorporated in a risk register.
- **Risk detection**—Unlike detection risk in a financial audit where the auditor concludes that no material errors are present when, in fact, there are, in the context of IS/IT risk management, this reflects the capability to detect that an unauthorized third party is attempting to penetrate a network or system (or has already successfully done so) in order to affect its availability, confidentiality or integrity.

  Many vendors specialize in the field of security information and event management (SIEM). The auditor should explore to what extent such products are relevant to the organization and, if they are, whether they have been purchased or plans to do so exist.
- **Contingency plans**—The CIO should own and update incident response and disaster recovery plans, which must be updated and tested constantly given the rapid pace of change in technical architectures. The plans should also be tightly linked to the organization's business continuity plans.

Risk Management System

The Committee of Sponsoring Organizations of the Treadway Commission's (COSO) *Internal Control—*

Enjoying this article?

- **Read *Risk Scenarios Using COBIT 5 for Risk*.** *www.isaca.org/riskscenarios*
- **Learn more about, discuss and collaborate on audit tools and techniques and risk management in the Knowledge Center.** *www.isaca.org/knowledgecenter*

Integrated Framework,[3] published on 14 May 2013, places a stronger emphasis on the importance of IS/IT and includes other enhancements within its principles.

In May 2014, ISACA® published a white paper[4] highlighting areas of alignment and differences in the content of the COSO and COBIT® 5 frameworks and presenting the complementary and compatible nature of their guidance.

If the COSO framework has been adopted for ERM, the auditor should validate that the risk management of IS/IT is appropriately aligned with it to ensure integration between them.

Extent of IS/IT Risk Management Integration in ERM

Given the relatively short time since the 2013 publication of the COSO framework and COBIT 5, the transition toward a more integrated environment can be expected to take some time as ERM organizations, internal audit, and the CIO and chief information security officer (CISO) learn and start applying the changes.

Given that different disciplines (e.g., finance) may use different standards and even different definitions and metrics of impact and risk, lack of integration may create gaps in understanding, incompatible assessments and difficulties in integrating the results. The auditor should examine the extent of integration and make appropriate observations; if necessary, the auditor may wish to recommend having a single integrated and prioritized source of risk information for the whole of the business.

Risk Monitoring

Risk monitoring can be active and reactive:

- **Active**—This should include risk intelligence, as already discussed, and inspection (or self-assessment), IS/IT audits and whatever corrective actions have been identified.
- **Reactive**—This consists of after-the-event actions to understand what happened and how, with the objective of learning about the vulnerabilities in people, processes and technology that caused it and drawing lessons from the incident in the hopes of preventing a repeat event.

  These actions include analysis and investigation and, while the outcome may cause discomfort, it is better to know. One little-publicized example was the way in which the Stuxnet malware was introduced into the high-security uranium enrichment facility at Natanz, Iran, and then into computers that were not connected to any outside network. In truth, the process involved people and a USB flash memory drive—an approach that was considered so unlikely that there may not have been a risk scenario (discussed in part 3 of this series of articles) seriously considered.

Risk Communication

Risk appetite is a core consideration in an ERM approach.

It can be defined as "the amount and type of risk that an organisation is willing to take in order to meet their strategic objectives."[5] Each organization needs to define it for different risk, relate it to the organization's sector of activity and culture, and express it in appropriate units (financial for impact, in minutes [or hours] for systems availability, etc.). While risk appetite means different things to different people, there is a consensus that a properly communicated, relevant risk appetite statement can help organizations achieve their goals and sustain their operations. This is hard to do, but without it, it is not possible to manage risk in any meaningful form.

The auditor should examine risk appetite statements relating to IS/IT for completeness and relevance and verify the extent of contribution and agreement from senior management.

Definitions

According to ISO 31000, risk is the "effect of uncertainty on objectives," and an effect is a positive or negative deviation from what is expected. The key word here is "uncertainty," as things are more than likely not going to go according to plan.

Many professions and activities have their own set of definitions of risk, and this can lead to misunderstandings, if not confusion. For example, a dialogue on risk between a medical surgeon and an investment banker, albeit unlikely, should be a facile illustration of mutual incomprehension.

The auditor should explore the extent to which the definition of risk used by IS/IT professionals is understood by the ERM team and other functions of the business.

Preliminary Conclusions

This article should not be seen as the end of the story, only its beginning. As the role of risk management increases in business importance there will be many more areas for the internal audit function to consider, such as the risk associated with data being discarded/destroyed, the use of encryption, single points of failure, and external suppliers and vendors. Part 3 of this article will discuss risk scenario planning.

Endnotes

[1] International Organization for Standardization, ISO 31000:2009, *Risk management—Principles and guidelines*, *www.iso.org/iso/home/standards/iso31000.htm*

[2] Apgar, David; *Risk Intelligence: Learning to Manage What We Don't Know*, Harvard Business School Press, USA, 2006

[3] Committee of Sponsoring Organizations of the Treadway Commission, *Internal Control—Integrated Framework*, 2013, *www.coso.org*

[4] ISACA, *Relating the COSO Internal Control—Integrated Framework and COBIT*, USA, 2014, *www.isaca.org/coso-and-cobit.*

[5] Rittenberg, L.; F. Martens; "Understanding and Communicating Risk Appetite," COSO, 2012, *www.coso.org*