IS audit basics

Auditing IS/IT Risk Management, Part 3

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.

The first two parts of this series of articles on auditing IS/IT risk management covered the audit of activities looking back in time to identify opportunities for improvement.

Given that risk is in the future, this column begins by examining the way in which IS/IT risk managers (in collaboration with the risk management function) look forward to try to anticipate risk factors and identify which will require mitigation plans (**figure 1**).

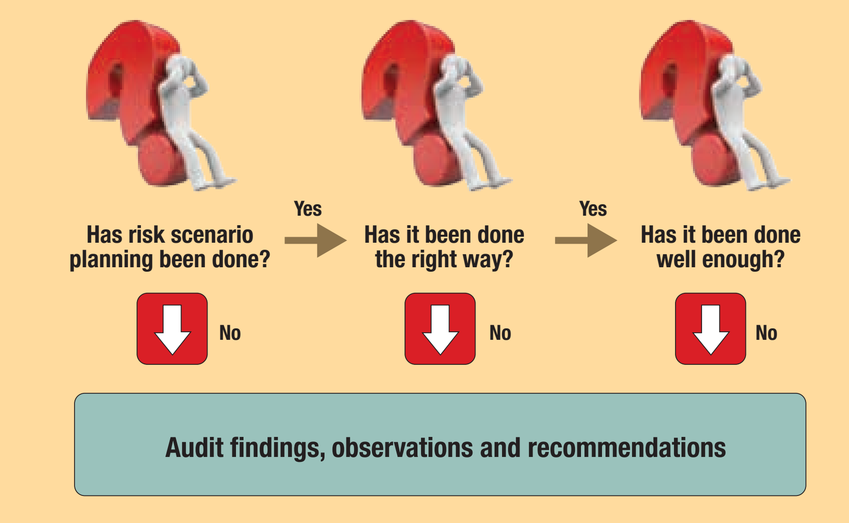
Risk (Scenario) Planning

The purpose and benefits of scenario planning are close to being self-evident. Undertaking risk scenario planning in the context of enterprise risk management (ERM) requires business managers and process owners, risk management specialists, the IS/IT function, and internal audit to collaborate because:

- Risk is in the future.
- It is not possible to mitigate risk without understanding possible events and how these affect projects and operational matters and their impact.
- Risk management makes little sense if you cannot distinguish the few areas of critical risk from the trivial many.
- IS/IT professionals can look only at internal risk, i.e., those directly relating to their domain of control.
- Business impact and, therefore, mitigation priorities relating to it should be owned by the appropriate business function.

There is adequate evidence that a growing number of organizations are taking the collaborative approach and applying established frameworks. However, the author’s personal observations made over many years reveal the contrary as well: Many organizations do not engage in these activities. A story related to this topic may prove enlightening. A shoe repairer posted a clearly visible notice in his shop. It said: “Cheap, Quick, Quality. You can choose any two.” In the author’s experience, cheap and quick are often the preferred senior management approach. When things go wrong, blamestorming can result.

Figure 1—Auditors’ Focus Areas


Has risk scenario planning been done?
Yes
Has it been done the right way?
Yes
Has it been done well enough?
No
No
No
Audit findings, observations and recommendations

Source: Ed Gelbstein. Reprinted with permission.

As discussed in previous articles in this series, the real difficulty is that, unlike other business areas (e.g., finance, foreign currency exposure), risk and risk appetite can be quantified.

In the case of IS/IT, there is a degree of confusion because of the scarcity of useful numerical data. For example, it is hardly helpful when the answer to a typical question such as, “What is the probability of a zero-day attack on product X from company Y?” is usually, “No idea.” If, instead, the question is raised as to its likelihood (a concept of relatively little value), the answer may be in terms of low, medium or high. The truth is that either it happens or it does not. Just like tossing a coin and asking if it will fall heads or tails, the probability is 50 percent, a number likely to make senior management very nervous.

The process for carrying out an exercise in risk scenario planning is particularly well described in chapter 5 of ISACA's *Risk IT Practitioner Guide*,[1] from which **figures 2** and **3** are particularly good summaries.

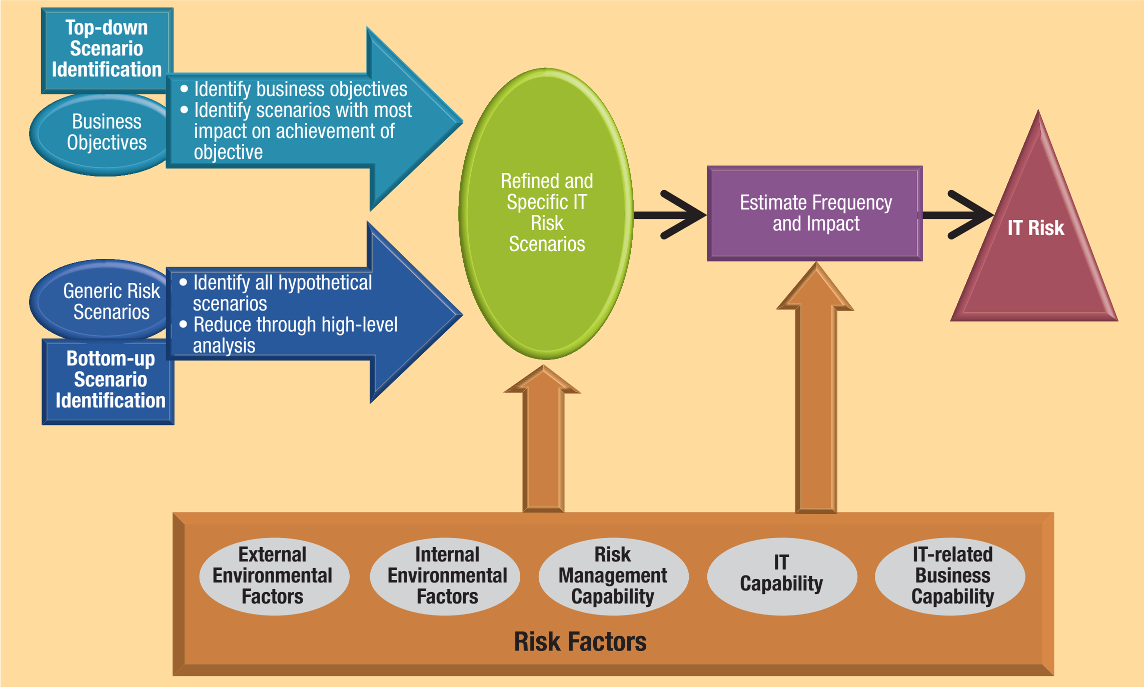
Please note that a key element here is the box labeled "Estimate Frequency and Impact," which often ends up as analysis paralysis because it is hard to reach agreement. However, if the scenario has already been described in the media, as a result of it having happened to someone else, it is a good indicator that the IT risk could be substantial.

As **figure 3** suggests, it takes more than a few minutes to develop a well-thought-out risk scenario: the process requires good knowledge of threats (actors and threat type) and vulnerabilities (asset/resource) as well as a guesstimate (there is no alternative word here) of the time to detect and fix. And all of this must take place before assessing the potential impact!

Given that most employees are facing heavy demands on their time—workload, pressure to deliver results quickly, interruptions, difficulties concentrating on complex problems, incomplete information, phone calls, meetings, etc.—it is not surprising that many give it a try and then ignore the issue or instead adopt a quick approach based on intuition (in reality, no more than guessing).

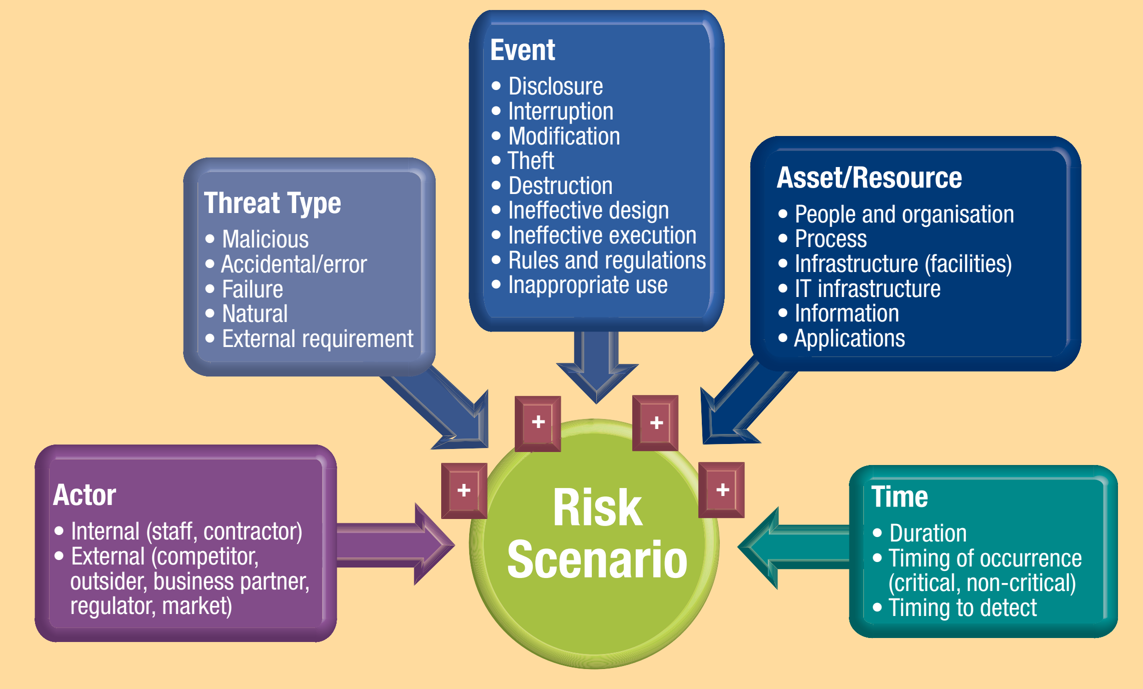
A recent article[2] in the *ISACA® Journal* makes an excellent companion to this column. It is

Figure 2—Steps in Scenario Development


Top-down Scenario Identification
Business Objectives
• Identify business objectives
• Identify scenarios with most impact on achievement of objective
Generic Risk Scenarios
• Identify all hypothetical scenarios
• Reduce through high-level analysis
Bottom-up Scenario Identification
Refined and Specific IT Risk Scenarios
Estimate Frequency and Impact
IT Risk
External Environmental Factors
Internal Environmental Factors
Risk Management Capability
IT Capability
IT-related Business Capability
Risk Factors

Source: ISACA®, *Risk IT Practitioner Guide*, USA, 2009

Figure 3—Components of an IT Risk Scenario



Source: ISACA, *Risk IT Practitioner Guide*, USA, 2009

interesting to note that the author adopted some of the preferred terminology of The Institute of Internal Auditors (IIA) when referring to "cause" and "consequence," but not "criteria," "condition" and "recommendation"—the remainder of The IIA's 5Cs.

The even more recent article on the benefits of risk scenarios[3] is also particularly good to review. Following are the key benefits cited in that article:

- A better understanding and management of IT risk in line with business objectives
- The positioning of security risk among other categories of IT risk
- The positioning of IT risk among the other categories of enterprise risk
- A better understanding of how to identify and manage IT risk
- An ability to communicate IT risk to business decision makers
- An identification of operational losses or development of key risk indicators (KRIs)
- A thorough consideration of real and relevant risk, not just threats and vulnerabilities

In addition, *COBIT® 5 for Risk*[4] is a highly recommended piece of work. The entire publication requires considerable time to be digested, but the product page included in the endnote contains a summary in the PowerPoint form that can be examined quickly and provides an overview of how the document is structured.

Main Challenges for the Audit Function

The blurring lines among the different roles of the risk management function and internal audit can cause conflicts of interest when audits are conducted on how risk management is carried out. After all, both functions are there to provide independent, well-thought-out information to senior management: the risk management function on what it has identified and assessed and on the ownership of the appropriate mitigation measures, and internal audit on the completeness, quality and effectiveness of the risk management methodologies and processes.

> **“The blurring lines among the different roles of the risk management function and internal audit can cause conflicts of interest.”**

The risk has to be owned by business process stakeholders and supported by risk managers and functional managers. Internal auditors, however, have the important responsibility of sharing risk foresight with senior management. If internal auditors are given the responsibility of the risk management function, they lose their ability to objectively advise the final decision makers and key strategists in making business decisions.

Conclusions and Other Things to Consider

It is part of the internal audit function to provide advice on risk to senior management and share insights with business process stakeholders. Ideally, this is done in collaboration with the enterprise risk management function and leads to a consolidated, prioritized risk register, in which mitigation measures are assigned ownership, time scales and, where appropriate, resources.

Internal auditors must not end up owning risk management. It is critical for auditors to maintain objectivity when auditing IS/IT risk management and make appropriate observations and recommendations where necessary.

Endnotes

[1] ISACA, *The Risk IT Practitioner Guide*, USA, 2009

[2] Power, B.; “Writing Good Risk Statements,” *ISACA Journal*, vol. 3, 2014, *www.isaca.org/Journal/archives*

[3] Young, L.; “Tips for Understanding the Benefit of Risk Scenarios,” *@ISACA*, vol. 25, 3 December 2014, *www.isaca.org/About-ISACA/-ISACA-Newsletter/Pages/at-ISACA-Volume-25-3-December-2014.aspx?cid=edmi_1105467&appeal=edmi#2*

[4] ISACA, *COBIT® 5 for Risk*, USA, 2013, *www.isaca.org/COBIT/Pages/Risk-product-page.aspx*