IS audit basics

Preparing for Auditing New Risk, Part 1

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

This is the first of two articles attempting something unwise: predicting future risk arising from information systems and technology. These pages are an invitation to readers to discuss them and suggest missing items, incorrect assumptions and how the role of auditors may change as a result.

Two quotations are especially apt: "Look to the future, because that's where you'll spend the rest of your life,"[1] and "The trouble with the future is that it usually arrives before we're ready for it."[2] Both apply to organizations taken by surprise before they can even consider issuing a policy and to everyone else (including auditors).

Innovative technologies have unintended consequences that become apparent after they have been adopted. Old-style audits were like driving a car by looking in the rearview mirror: They concentrated on past actions, looked for faults and recommended improvements. Now there are risk-based audits, which rely on acceptance that risk is in the future and collaboration with those identifying and assessing risk is the most effective approach.

Doing this strengthens the consultancy role of internal audit by opening a dialog with the risk function, data custodians and information systems/information technology (IS/IT) operations, and raising awareness with senior management. Accountability for following up and mitigating emerging risk remains with the auditees.

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.

It is also necessary to accept that attackers are smart, hard-working and possibly more motivated than the defenders. Attackers have fewer challenges to contend with such as administrative trivia, justification of expenditures, organizational politics and lack of senior management interest.

Attack tools continue to become more sophisticated and data assets more valuable and critical. All of these factors make thinking about future risk more important than ever.

Evolving Domains of IS/IT and Their Potential Risk: The "Known Knowns"

Auditors are not accountable for risk management or assessment, but it is appropriate for them to take an interest in developments likely to change their organization's exposure to risk. An initial list—readers are invited to suggest additional items—includes the items outlined in **figure 1**.

Figure 1—Overview of Emerging IS/IT Risk Domains

Known Knowns	Known Unknowns
Governance	Internet of Things
Mobile	Big Data
Cloud	Militarization
Software	Over the Horizon

Source: E. Gelbstein. Reprinted with permission.

Governance Audit Challenges

Board members and senior managers (the C-suite) have a broad range of responsibilities, huge demands for their time and attention and, inevitably,

a limited knowledge of many corporate disciplines. IS/IT are probably the ones they know the least about.

> **IS/IT is ubiquitous in any organization and may create an illusion of intuitiveness and simplicity, neither of which is true.**

Chief information officers (CIOs) are seldom part of the C-suite and, when things work, IS/IT becomes invisible. That is, until budget time, at which time the "Why are we spending so much on this?" issue is raised. Because information is intangible, quantifying the return on investment (ROI) of IS/IT remains a challenge.

This is unfortunate because both strategy (and the res that support it) and policies[3] need the informed participation and commitment from the executive level. This can lead to two potential negative outcomes:

1. Policies[4] are not issued before the lack of them creates an irreversible situation (as happened in many organizations with social media and bring your own device [BYOD]).
2. When policies are issued, they are not understood or complied with in day-to-day activities.

IS/IT is ubiquitous in any organization and may create an illusion of intuitiveness and simplicity, neither of which is true. The chief audit executive (CAE), the IS/IT auditors and the audit committee are well placed to convey these messages to the leadership of the organization and address them at the strategic level.

The Audit Challenge of the Mobile World

Developments in mobile technologies have occurred faster than many expected; even some vendors were taken by surprise (and went out of business). The reality now is that smartphones, phablets and tablets are rapidly displacing the easier-to-control environment of networked personal computers, thus introducing new risk to the organization.

Individually owned devices used to access corporate data should be of concern to auditors because, at a minimum, the following may occur:

- Nobody is accountable for the security of the devices—not the chip designers and manufacturers, the operating system designers, the designers of applications (apps), network operators, Internet service providers, or others.
- Owners of mobile devices can easily learn how to remove restrictions placed by their vendors,

Enjoying this article?

- **Read IT Risk Management Audit/Assurance Program.** *www.isaca.org/auditprograms*
- **Learn more about, discuss and collaborate on audit tools and techniques in the Knowledge Center.** *www.isaca.org/it-audit-tools-and-techniques*

"jailbreaking" in iOS devices and "rooting" in Android devices. This is a form of privilege escalation, i.e., a method to gain access to resources that are normally protected from an application or a user. This leaves the device open to cyberattacks and the leakage of sensitive information.

- Countermeasures against the loss or theft of a device accessing sensitive corporate data or malware fall into two categories: building greater awareness of good practice to protect their devices and the data they contain (good hygiene)[5] among owners/users and using products such as antimalware detection and protection. It is questionable to what extent these are implemented.
- Because of the reliance on such devices, auditors should discuss with the executive level whether mobile devices should be included in disaster recovery and business continuity plans. However, at present, this is rarely the case.
- Legislation on individual rights concerning privacy may not allow an organization to monitor or audit such devices and this leaves the organization exposed to unknown risk.

Among the high-impact developments to be expected in the mobile world is an enterprise app store providing certified software, data visualization, predictive analytics and augmented reality; in fact, these offerings are already on the horizon. Is it possible to predict what will come after them?

Outsourcing and Cloud Services

While outsourcing has been around for many years and is well understood, the growth of cloud usage has been faster than many expected and data have migrated[6] to this environment before data owners could give due consideration to the implications of doing so. Given that operational accountability has been transferred to a third party, this can create the "out of sight, out of mind" reaction.

Corporate businesses store sensitive personal and proprietary information in the cloud. However, their contractual arrangements may not have adequate provision for auditing how the service provider protects this information against unauthorized access by third parties and by their own personnel.

The case for assessing this individual risk and how to do so (if it is at all possible) should be discussed with the service provider, and the discussion needs to reflect the criticality and sensitivity of the data concerned. This risk could change rapidly if and when there is a consolidation of the market for cloud service providers involving mergers, acquisitions and disposals.

These issues add to the already long list of things auditors need to consider including in their audit strategy and audit plans related to the cloud.

> **"Risk could change rapidly if and when there is a consolidation of the market for cloud service providers involving mergers, acquisitions and disposals."**

Software

This topic is so large it could fill a book. The following provide only a high-level view:

- **End-user computing (EUC)**—This includes spreadsheets, personal databases and small applications. No one knows exactly what is "out there," undocumented, untested and possibly of questionable quality. This does not stop these files being used to support critical business decisions.
- **Apps for mobile devices**—Apps are easy to buy, download and install, but they can also introduce embedded malware. In addition, suppliers of the devices add apps that the buyer cannot remove. Users who jailbreak their devices create additional risk. These are all hard to audit and present unknown risk.

- **Conventional off the shelf (COTS)**—Shrink-wrapped and/or customizable software such as enterprise resource planning (ERP) and customer relationship management (CRM) will not be discussed in this article because they have been around for a long time and, therefore, have been extensively audited.

Custom software[7] has specific audit needs including built-in controls (e.g., access controls, privileges, segregation of duties) and toxic code back doors, logical bombs or other features programmers can exploit at will. Auditors are well aware of these issues.

Programming techniques such as service-oriented architectures and the emerging software-defined architecture cannot be audited without substantial knowledge of what they involve—another challenge for the auditors.

Interim Conclusions

This column discusses the "easy" aspect of new risk. By now, we should have recognized these aspects and started to audit those areas for which there are guidelines (admittedly, not many). Part 2 of this series will focus on more speculative items.

Endnotes

1 George Burns, 1896-1996, US comedian, actor and producer
2 Arnold H. Glasow, 1905-1998, US businessman
3 Lyra, M. R.; J. C. F. Simoes; "Checking the Maturity of Security Policies for Information and Communication," *ISACA® Journal*, vol. 2, 2015, *www.isaca.org/Journal/archives*
4 IBM MaaS360, "Bring Your Own Device—Ten Commandments," *www2.maas360.com/services/maas360-ten_commandments_of_byod_bring-your-own-device.php*
5 Gelbstein, E.; "Imperfect Technologies and Digital Hygiene: Staying Secure in Cyberspace," *ISACA Journal*, vol. 5, 2014, *www.isaca.org/Journal/archives*
6 Gelbstein, E.; V. Polic; "Data Owners' Responsibilities When Migrating to the Cloud," *ISACA Journal*, vol. 6, 2014, *www.isaca.org/Journal/archives*
7 A three-part IS Audit Basics Column, "Large Software Projects," will cover this topic and are to be published in upcoming issues of the *ISACA Journal*