Perspectives From a Seasoned Practitioner

Ed Gelbstein, Ph.D., has worked in IS/IT in the private and public sectors in various countries for more than 50 years. He 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 1990s, 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. He also teaches postgraduate courses on business management of information systems. He can be contacted at *gelbstein@diplomacy.edu.*

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 choose the Comments tab to share your thoughts.

Go directly to the article:

It was a bit of a surprise and a huge compliment to be invited to contribute to this column after many years reading the words of Tommie Singleton in this space. I shall do my best not to disappoint. To give you a hint as to where this column is going during the upcoming year, let us start with a summary of some lessons learned in my many years dealing with information systems, technologies and audits.

Change is fast and profound. Over the last five decades, technical innovation and new legislation relating to data and information have caused major dislocations. These, in turn, have created the need for new approaches to IS/IT audit. Some of these changes are outlined in **figure 1**.

While this table is certainly incomplete, the conclusion is that continuous learning is inescapable. Thus, we are required to learn how to learn and then how to unlearn and relearn.[1] Failure to do this is a guarantee of professional stagnation and failed careers.

In the IS Audit Basics column, I plan to reflect the lessons I learned both as an auditee and as an IS/IT executive and auditor. I intend for them to be thought-provoking as opposed to sets of procedural "do this" statements.

WHAT WE KNOW WE KNOW

Dependency on IS/IT has become irreversible and its governance and management rely on audit competencies and independence. Innovation cycles are likely to remain short and bring with them new vulnerabilities and management challenges.

Besides, internal and external threats keep changing and, unless mitigated, these could have an adverse and potentially serious effect on organizations. The frameworks for information assurance, security, risk and governance evolve as experience is gained and lessons are learned.

The same is true for audit standards and guidelines. It is prudent to assume that the domains of IS/IT audit have become so large that it is now unlikely that anyone can know everything about it. This makes the development of IS/IT audit strategies that much harder.

On the positive side, the audit profession offers many opportunities for personal and professional growth: progression to chief audit executive (CAE), membership in audit committees, consultancy and senior management roles. The choice is yours, but only if you are prepared.

Figure 1—Historical Timeline of Data-related Technical Innovation

The 1960s	Migration from analog to digital, emergence of digital, integrated circuits; IBM 360 series of mainframes; minicomputers from many vendors; SCADA used in industrial control; proliferation of programming languages (e.g., ALGOL, COBOL, FORTRAN, BASIC). Data speeds were 2.4 kbps at best and fax machines Group 2.
The 1970s	Transaction processing becomes the norm; early cellular data communications and optical fiber networks; Internet email and early personal computers; BASIC becomes widespread.
The 1980s	First 16-bit PCs; local area networks (LANs) enter the corporate world; packaged software for office applications becomes available from several vendors; malicious software (malware) appears. Firewall products on offer; data protection legislation is introduced in the UK.
The 1990s	Client-server claims "the mainframe is dead"; graphical user interfaces become ubiquitous; executive awareness of the critical dependence on IS/IT; Internet access makes its way into enterprises; web 1.0 grows explosively; pioneers enter e-commerce; European Data Protection and US Heath Insurance Portability and Accountability Act (HIPAA) legislation are enacted; Y2K becomes a concern.
The 2000s	Technology users become proficient; malware becomes professional; COBIT 3rd Edition is published and widely adopted; social networks' popularity gives rise to corporate issues. Mobile technologies are transformed by smartphones and tablets; bring your own device (BYOD) and mobile apps become an enterprise issue. Risk-based audits are widely adopted.
The 2010s	Cloud computing; big data; concerns about the theft of intellectual property; threats to individual privacy and the militarization of cyberspace; the Internet of Things (IoT) and wearable technologies. COBIT® 5 covers several volumes of guidance and separates governance from management.
Beyond	Who knows?

The following is a good reminder of what the concept of "auditor" covers:[2]

- A.....Analytical
- U.....Unbiased
- D.....Diplomatic
- I.....Independent (and inquisitive)
- T .....Thorough
- O.....Objective
- R .....Reliable

Having worked with (and learned much from) many capable auditors, there have been occasions when I came across others who would have done far better to have pursued a different career. Why? Because they showed themselves to be one or more of the following: arrogant, disorganized, undisciplined, opinionated, cynical or emotionally incontinent. Let us say that they were not respected by their victims.

YOUR CREDIBILITY AND OTHER GOOD THINGS OF WHICH TO BE CONSCIOUS

Credibility is *the* essential asset for any auditor. If your independent assessments cannot be backed by your credibility, they are worthless and, therefore, as an auditor, so are you. Credibility is built over time by developing knowledge and experience. It helps to:

- Fully understand what your CAE considers to be "good enough"
- Make certain at all stages that anything you say and write is supported by evidence—be it audit tests that you have personally conducted or documentation you have reviewed
- Maintain confidentiality by discussing audit findings and results with only those who need to know
- Remember that gossip, rumors and other inside information are not evidence
- Not jump to conclusions

Integrity is another fundamental requirement for an auditor, involving honesty, fair dealing (or objectivity) and truthfulness.

Finally, after passing the Certified Information Systems Auditor® (CISA®) examination, you are likely to be dealing with experienced professionals from whom you can learn much. Make sure you take the time to do so, as this is the best way to broaden your understanding and experience of the audit process and the interpersonal and political dimensions of the job. Ask lots of questions, particularly "Why?," until you are satisfied with your understanding.

It is good to remember that while management understands the role and importance of audits, when the time comes, auditors are rarely welcome. After all, when the auditors descend on a team carrying out project or operational work, the result is disruption: The auditors need documentation and access to data, request meetings over a period of several weeks or more, and keep asking awkward questions.

Bear in mind that some auditees may have had bad experiences if previous auditors created the impression that they were focused on criticism, assigning blame or engaged in the mindless pursuit of perfection. Besides, if members of previous audit teams were not well informed about the role of IS/IT in the organization—its criticality, structure, resources, past performance and related issues—they may have been perceived as not making good use of the time assigned in the audit plan or focusing on irrelevant areas.

It is important for auditors to understand the auditee's history: What was the scope of past audits? What actions were recommended (particularly those worded "shall" rather than "should")? And, how many of these implementations were re-audited? It is also important to find out how many of the recommendations were not implemented and why.

Knowledge of the audit history should include the approach taken by your predecessors, the audit strategy, the adopted standards and guidelines, and, especially, the interpersonal relations between past auditors and auditees. A history of disagreements, conflict and lack of trust is hard to recover from and can easily result in mistrust and resistance.

ABOUT THE NEXT COLUMN

The next column will continue this introduction to the realities of IS/IT audits by exploring what makes an audit successful from the perspective of the many parties involved: the auditors, the CAE, the audit committee, senior management and, not least, the auditees.

Given that audits are an activity carried out by people who interact with other people, topics related to soft skills will appear in future columns because successful audits depend on how such interactions take place.

CONCLUSION

You can be confident that IS/IT technologies will continue to change and with them, audit practices. Be prepared!

ENDNOTES

[1] Alvin Toffler, *www.alvintoffler.net/?fa=galleryquotes*

[2] Tangient, "Introduction to Audit," boruetthsm, *boruetthsm.wikispaces.com/file/view/Auditing.ppt*