IS Audit Basics

Ed Gelbstein, Ph.D., 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 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. 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 choose the Comments tab to share your thoughts.

Go directly to the article:

Trust, but Verify

"Trust, but verify" is a Russian proverb that became more widely known when then-US President Ronald Reagan used it in the 1980s. (*Доверяй, но проверяй [doveryai, no proveryai*]). The fact that proverbs are passed unchanged through generations implies that they are seen as the truth.

TO RE-AUDIT OR NOT TO RE-AUDIT

The auditors arrive, do their work, write a report that includes critical recommendations that could be seen as an instruction: "...the auditee shall...."

Should the audit strategy and planning call for a review (e.g., one year after issuing the final report) to see if they have been implemented and, if so, whether the implementation has been completed in a way that significantly reduces business risk?

> "The audit universe has become so large that re-auditing issues are bound to conflict with the overall audit plan."

While this makes good sense, the challenge is that the audit universe has become so large that re-auditing issues are bound to conflict with the overall audit plan.

THAT UNWELCOME FEELING

Many auditees mistrust the auditors: Their findings are the equivalent of calling the auditee's baby "ugly." No parent would ever do this, but then, there are ugly babies. Therefore, unless a good working relationship has been established over the years, the auditor cannot expect a warm welcome or for the auditees to share their problems and concerns.

A poor welcome could include finding that the auditors have been assigned poor accommodations, possibly in an inconvenient location, limited support facilities (e.g., printers, photocopiers, locked doors and cabinets, shredders), an unhelpful contact point or discovering on short notice that a critical person is not available for discussions.

There will be many plausible excuses. It is never a good time to conduct an audit and accommodation is an issue almost everywhere. If the arrangements are really poor, it may be good to have the chief audit executive (CAE) speak with a senior manager who can act to resolve the issue and understand the root cause of the situation.

THINGS AUDITEES MAY "FORGET" TO DISCLOSE

A competent and experienced information systems (IS) manager would be expected to anticipate what the auditors may find by conducting a brutally honest assessment of the many aspects of IS and IT. Guidelines and frameworks such as COBIT® 5 can facilitate this task. In practice, this does not happen often as other activities, deemed more urgent, displace these and before you know it, it is audit time again.

If the auditee can demonstrate to the auditor that they care about the audit process; that they understand how it is conducted; and then come up with a list of findings, observations and corrective actions by themselves, the relationship would be strengthened and it would make better use of the auditor's knowledge and experience. The downside of keeping information from the auditors is that they will find out by chance or by process.

In one example, there was a wiring cabinet in an office environment for a critical network that the "owner" had known for years consisted of spaghetti cabling, equipment on the floor and a tree of extension leads. This was not mentioned at the start of the audit, but as the auditors were passing by, someone opened the cupboard door. A photograph of the scene was included in the draft and final audit reports, despite requests for its removal.

LOOK AND LISTEN

The examples in the previous section show carelessness and incompetence, but not malice. Unfortunately there are many more things that the auditees know that their management does not. This becomes an explosive issue when it involves the means to work around sound policies (e.g., need to know, least privilege, segregation of duties, change management). Here are some examples collected over many years.

A homemade, old (e.g., COBOL) financial application was made Y2K-compliant and fully met the needs of the organization. It was robust, reasonably well documented and maintained by a small team that had done so since the initial design. During an audit that did not involve this application, it was discovered that the lead developer had embedded undocumented hidden accounts and backdoors, not to be abused, but to "help" the organization toward bypassing the usual controls. And, there was no record of who had what access controls and privileges or if any were kept by individuals as their careers progressed. Furthermore, weak change control supported these changes.

The lead designer was due to retire, and once the auditors became unofficially aware of this, the question arose as to whether a colleague months or years away from retirement should hold the "secret" of these unofficial features. The management view was a clear *no*, and the system was retired and replaced by a commercial application with role-based access controls and more manageable superuser features.

Superuser privileges can be a problem. In another case at a different organization, the design of an enterprise resource planning (ERP) system had a project manager who assigned himself extensive superuser rights. After the project was completed, nobody thought to verify what rights were retained by the implementation team.

An even more extraordinary situation happened when a senior executive at an organization instructed that all security policies be withdrawn and the organization's data be declassified in order to be fully transparent. Neither internal audit, risk management or legal counsel were consulted and nobody was willing to say, "The emperor has no clothes."

SERENDIPITY

Sometimes one has the good fortune of coming across something interesting without looking for it. Here are some examples.

- **The invisible single point of failure**—A law enforcement unit (in the 1980s) was implementing a new secure network of leased lines. The service provider designed it to ensure that different cable routes provided resilience. Surprise! The two leased lines entered the building through a single point accessible through a manhole in the street just outside the main entrance.
- **External audit of a large and complex information systems and technology department**—During an audit, the systems architecture, i.e., how applications exchanged data with other applications—with or without format conversion, dynamically, by file transfer—was requested. Lo and behold, it had not been documented. There was no comprehensive systems architecture listing, for example, the name of the system, its custodian, purpose, high-level functionality and interfaces. Moreover, there was no statement about the system's condition (e.g., robust, well documented, frozen) and planned activities. This led to an unplanned question about the data architecture, as the audit team tried to understand how many data entities were duplicated across systems (in incompatible formats, of course), and this was received with a "not in my job description" response.

> "There is much to be gained from an open, collaborative relationship between auditors and auditees."

- **Hidden or forgotten opportunities**—In fact, there is plenty out there neatly hidden or forgotten, including software licenses that are paid for, but not used; large, over-optimistic and underresourced projects; renewals and upgrades postponed until the service deteriorates, bypassing procurement rules; critical activities for which there are no backups for the responsible individuals; and unqualified individuals (e.g., interns or trainees) doing things beyond their capabilities. Some are due to weak management or political posturing (e.g., "It is my budget and I will do it despite what you say."); others are caused by SMRC (saving money regardless of cost), also referred to as "shareholder value."

CONCLUSION

There is much to be gained from an open, collaborative relationship between auditors and auditees in which both parties focus on understanding and managing business risk. Rationally, we all know this is the case, but human factors such as lack of trust and organizational politics often get in the way.