IS Audit Basics

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 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. Gelbstein also taught postgraduate courses on business management of information systems.

Auditors and Large Software Projects, Part 1

Can Auditors Prevent Project Failure?

Large software projects have been notorious because of:

- Their large budget and timescale overruns
- Failing to deliver the promised benefits
- Being accredited to production before they are ready (insufficient testing, inadequate documentation and everything in between)

How can this happen, given that this has been known for many years and there are many methodologies and sources of guidance available to software developers and project managers? Examples include PRINCE 2,[1] the Project Management Body of Knowledge (PMBOK)[2] and the Software Engineering Body of Knowledge (SWEBOK).[3] Moreover, many of the professionals involved in this work hold certifications from the Project Management Institute and/or the SWEBOK certificate.

Auditors also have many sources of good practices and guidance such as ISACA's own *Systems Development and Project Management Audit/Assurance Program*[4] and the guidelines for auditing IT project management published by The Institute of Internal Auditors.[5] There is also a worthwhile *ISACA® Journal* article on project risk management.[6]

Even though many projects have been "audited to death," the problem persists to the extent that the Working Group on IT Audit of the International Organization of Supreme Audit Institutions (INTOSAI) dedicated an issue of its journal to the topic of "Why IT projects fail,"[7] and more articles on this theme continue to appear. The catalog of failed projects is huge. "Failure" is a flexible word that can mean different things to different people, e.g., a three-month delay to a project may not be considered a failure in some cases, yet is an absolute disaster in others.

HOW CORPORATE LIFE CONSPIRES TO CAUSE AN IT PROJECT TO FAIL

Having participated in a few successful large projects years ago and also witnessed (and in some cases audited) projects that failed, some were abandoned when management had the opportunity and courage to do so. However, this is not always the case, and money and people can continue to be thrown into a failing project's black hole.

This column explores some of the realities surrounding failed projects. The sections and findings presented are a composite of findings from several projects over many years (and they keep turning up). No identities or details of the project owners are given because of nondisclosure agreements signed to protect their confidentiality.

The Business Case

Large projects fall in two categories:

- Replacements or major enhancements to an existing system (which is, therefore, known and understood)
- Innovative solutions that create opportunities for change and, therefore, are somewhat speculative

The auditor should always request and study the business case.

The business case for the first category would be based on the shortcomings of the existing system and how these would be overcome by

Editor's Note

On 19 July, 2015, Ed Gelbstein, Ph.D., passed away after a lengthy illness. He was a prolific writer and contributor to the ISACA Journal *and a valued and admired colleague. His work will continue to be published in the* ISACA Journal *posthumously.*

FORUM

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:

the proposed project. The auditor could consider reviewing the technical risk of a system that may not be properly documented or may be fragile because of other reasons.

This may not be all that hard to do, except for the limited ability to predict costs with reasonable confidence. Such estimates do not have a particularly good track record.

Innovative solutions are more of a crystal-ball-gazing exercise, and estimated costs and benefits may be inaccurate at the time of doing the business case.

One example of where this proved to be problematic involved a large database for sensitive personal information. Consultants were engaged to estimate the benefits that could be expected and produced a series of glossy reports with impressive numbers.

The audit finding: The reported estimates were suspiciously accurate—down to 1 euro in zillions and years away from being achieved. The reports did not include the assumptions made to support the benefits and presented only a best-case scenario. There was no mention of a most likely or worst-case scenario. The costs were a guess, not even an educated one. The sponsor was not happy with the auditor's observations but decided to shelve the project.

The Project Risk Analysis

The auditor should request and study reports that define business risk, project risk and technical risk, assuming these definitions have been created (not always the case), and determine if the risk assessments are based on a proper methodology.[8]

Many years ago, a large project was launched without any risk analysis created and it went off the rails within a short time. The client believed that the vendor would be responsible for the management of the project. The vendor was, but only as far as its responsibilities extended. The client did not think it was necessary to have a project manager. It took two years to put the project back on track.

An often-ignored project risk is assuming that the project manager could be guaranteed to be there for the many years of a project. Wrong. Some gave up (see the upcoming part 2 of this article, to be released in vol. 3, 2016); others were offered a better job elsewhere and left. Finding a person capable of taking over once the project has started and leading it to a successful conclusion may be harder than it looks.

Other easy-to-ignore technical risk relates to the rapid obsolescence of the technologies initially selected, plus limited knowledge of the products that replace those technologies; the disappearance of a supplier because of bankruptcy, mergers and acquisitions; or, less frequently, the supplier's decision that the product is no longer viable.

This happened to the biggest civilian IT scheme attempted for the UK National Health Service. The project had been in disarray since it missed its first deadlines in 2007. The project had been beset by changing specifications, technical challenges and clashes with suppliers, which left it years behind schedule and well over budget. Accenture, the largest contractor involved, walked out on contracts worth £2 billion in 2006.[9]

The Requirements Definition

The auditor should review the stages through which the functionality and features that the system should deliver were developed and report the appropriate findings. What should go into a requirements definition is well defined elsewhere, but this does not mean it actually happens. Nonetheless, the auditor should give particular attention to the sections in the requirements definition that address key system controls, such as measures to ensure segregation of duties (SoD); the methods for granting and controlling privileges including role-based access controls; and management of superuser rights, logs, and audit trails.

Beyond this point, the auditor should consider recommending that any changed or additional requirements once the system design and estimates have been frozen should be allowed only if there is an overwhelming reason for doing so, and then, strict change control should be applied.

CONCLUSIONS

This column, the first of three, focused primarily on those aspects of project management of large software developments that, if not done well enough, contribute to budget and timescale overruns or, at worst, the failure of the project.

Smaller projects, such as those classed as "end-user computing" rarely get the benefit of an audit, even when they consist of sophisticated spreadsheets that are, in fact, a complex software project and are used for critical analyses. It is not uncommon for these to be undocumented and poorly tested, perhaps an issue for a future column, as is the whole topic of software quality.

ENDNOTES

[1] AXELOS Ltd., Prince2, *www.prince-officialsite.com/*

[2] Project Management Institute, Project Management Body of Knowledge (PMBOK), *www.pmi.org/PMBOK-Guide-and-Standards.aspx*

[3] IEEE Computer Society, *Guide to the Software Engineering Body of Knowledge, www.computer.org/portal/web/swebok*

[4] ISACA, *Systems Development and Project Management Audit/Assurance Program*, 2009, *www.isaca.org/auditprograms*

[5] Mookhey, K. K.; "Auditing IT Project Management," The Institute of Internal Auditors (The IIA), 1 May 2008, *https://iaonline.theiia.org/auditing-it-project-management*

[6] Singleton, Tommie; "What Every IT Auditor Should Know About Project Risk Management," *ISACA Journal*, vol. 3, 2004, *www.isaca.org/archives*

[7] INTOSAI, "Why IT projects fail," *The IntoIT Journal*, iss. 26, May 2008, *www.intosaiitaudit.org/publication_and_resources/1*

[8] *Op cit*, Singleton

[9] Wright, Oliver; "NHS Pulls the Plug on Its £11bn IT System," *The Independent*, 3 August 2011, *www.independent.co.uk/life-style/health-and-families/health-news/nhs-pulls-the-plug-on-its-11bn-it-system-2330906.html*