EDPACS
THE EDP AUDIT, CONTROL, AND SECURITY NEWSLETTER

JANUARY 2011 VOL. 43, NO. 1

AUDITING IT PROJECTS: EARLY WARNING SIGNS OF MATERIAL RISK

LEON A. KAPPELMAN

Abstract. IT projects are often materially significant and yet the nature and magnitude of their risks go unnoticed until disaster strikes. Significant problems and failures associated with IT projects are largely avoidable if one knows how to spot the signs of impending difficulty. The importance of auditors, if they know what to look for, in helping management see IT project risks and thereby preventing both large and small disasters cannot be over estimated. Focusing on the early warning signs of IT project peril, this article provides a straightforward starting point for seeing, monitoring, auditing, and managing the risks of an IT project.

WHAT YOU DON'T KNOW CAN HURT YOU

A ship is safe in harbor, but that's not what ships are for.
—William Shedd

Information technology (IT) investments comprise about half the capital budgets of U.S. organizations (Carr, 2008). Yet many IT projects are cancelled, completed late, exceed budget, or fail to deliver the promised business capabilities and financial return on investment (ROI). The planning and management of IT system investments and the projects that implement them can often be material concerns for organizations because of (1) the relative size of the investment itself, (2) the operational and thereby financial risks of the project, and/or (3) the control implications of the new system. Such IT projects can be of particular significance for SOX (the Sarbanes-Oxley Act of 2002), SAS 70 (the Statement on Auditing Standards No. 70: Service Organizations), financial forecasts, Securities and Exchange Commission (SEC) reports, and other regulatory and reporting requirements (Singleton, 2010; Gonzales, 2008). Moreover, such concerns are not limited to U.S. companies and their foreign subsidiaries since such risks and these laws and standards potentially affect companies outside the United States, as

IN THIS ISSUE

Taylor & Francis
Taylor & Francis Group

well as government and not-for-profit organizations, too. Given the magnitude of the resources utilized, the opportunity costs, the financial and operational materiality, and the risks involved, IT projects are not only an issue for the attention of Chief Information Officers (CIOs) but clearly for auditors, Chief Executive Officers (CEOs), Chief Financial Officers (CFOs), boards of directors, and other executives as well.

The management and mastery of risk distinguishes modern times from the past (Bernstein, 1996). IT project management, despite the fact that it deals with "modern" technologies, is embarrassingly immature in the mastery of risks with about 20% of IT projects cancelled before completion, nearly half with cost or time overruns or failing to fully meet requirements, and thus only about a third finished on-time, within-budget, and with expected functionality (Standish Group, 2006). If the discussion is limited to larger and therefore riskier projects, yet still only about half the size and capability of the software on a fresh new Apple iPhone®, the total-failure cancellation rate approaches 50% (Jones, 2009). Obviously, more effective risk management is needed to avoid troubled IT projects and make desirable risk taking possible.

IT projects are often materially significant and yet the nature and magnitude of their risks go unnoticed until disaster strikes. A few examples of the financial impacts of troubled IT projects include (Nelson, 2007; Charette, 2005):

- a retailer's restatement of five years of financial reports due to flawed software;
- the bankruptcy of a $5 billion medical wholesaler as a result of defective billing software;
- a manufacturer unable to ship several hundred million dollars in merchandise during its busiest season because of a late software project;
- a car manufacturer's recall of 20,000 vehicles to install a software fix in order to correct stalling problems;
- improperly tested software causing a privacy breach of the personal information of several hundred thousand customers of a financial organization; and
- the stock of an insurer dropping over 60% due to billing system failures resulting in the destruction of $3 billion in market capitalization, receivables write offs of more than $100 million, and multi-million dollar fines levied by government agencies.

If you have information of interest to *EDPACS*, contact Dan Swanson (dswanson_2008@yahoo.ca). *EDPACS* (Print ISSN 0736-6981/Online ISSN 1936-1009) is published monthly by Taylor & Francis Group, LLC., 325 Chestnut Street, Suite 800, Philadelphia, PA 19106. Periodicals postage is paid at Philadelphia, PA and additional mailing offices. Subscription rates: US$ 334/£202/€268. Printed in USA. POSTMASTER: Send address change to *EDPACS*, Taylor & Francis Group, LLC., 325 Chestnut Street, Suite 800, Philadelphia, PA 19106.

THE CRITICAL ROLE OF AUDITORS

Risks always have to be taken; it's merely a question of which ones at any particular time.

—Hal Clement

Such significant problems and failures associated with IT projects are largely avoidable. The importance of auditors in helping management see IT project risks and thereby preventing both large and small disasters cannot be over estimated. And the earlier in the life of a project that auditors get involved the better (Hettigei, 2005). "Auditors should play an important role in ensuring that IT investments are well managed and have a positive effect on an organization. A well managed IT project is absolutely critical to this success" (Swanson, 2010, p. 129).

A well staffed Project Management Office (PMO) and competent project personnel are also important in this regard; however, nearly all such activities are located within the IT department and report to the CIO. Although this is not necessarily problematic, independent and effective monitoring of IT projects by skilled auditors reduces both the appearance and actuality of partiality. The degree of auditor engagement in a particular project is of course a function of many factors including the level of financial, operational, and/or strategic materiality as well as the amount of project risk (given parameters such as size, cost, complexity, and duration). It also "depends on the risks involved and the assurance requirements of the board and executive management" (Swanson, 2010, p. 130).

SEEK AND YOU SHALL FIND

Strive to manage risk while trying to exploit opportunity.

—Peter Mauthe

The post-mortem examination of failed IT projects reveals that long before the failure there were significant symptoms or "Early Warning Signs" (EWSs). This article describes the most important EWSs of IT project failure based on a research project conducted by the author and his colleagues. Fortunately such EWSs are easily identified if one knows what to look for and once identified appropriate action can be taken to mitigate their impact.

To qualify as an EWS for the purposes of this research the indicator had to be identifiable in the first 20% of the project's original calendar. It is true that many of the EWSs can and do manifest much earlier than the 20% mark, even before a project is approved and funded, and should be dealt with at that time. Other highly important EWSs typically cannot manifest until after approval and funding as, for example, personnel are assigned and start dates finalized. The choice of 20% is consistent with the research goal of identifying all those risks that can manifest while it is still early enough in the project's lifecycle to take corrective action before too much damage is done (Hay, 2003). This focus on EWSs, instead of general IT project risks, aims to help auditors, CFOs, CIOs, project managers, and other stakeholders take action while

the project can still be saved at a reasonable cost. Alternatively, a risk-reward determination may indicate the project is no longer needed or unlikely to deliver a sufficient ROI and should therefore be cancelled before further resources are wasted.

First the academic and practitioner literature was searched extensively to develop a preliminary list of EWSs. Then a panel of 19 IT project management experts assessed the list adding and modifying items resulting in a list of 53 EWSs. Then 138 experienced IT project managers were invited to rate the 53 EWSs using a scale from 1 (extremely unimportant) to 7 (extremely important) in order to identify the most important EWSs of IT project failure (Kappelman, McKeeman, & Zhang, 2009). Although only summary results are reported here, the entire list of 53 EWSs is provided in the Appendix and complete details of the research is available in the article by Kappelman, McKeeman, and Zhang.

THE FOUR HORSEMEN OF IT PROJECT DOOM AND THE DEADLY DOZEN EWSS

> *The act of discovery consists not in finding new lands but in seeing with new eyes.*
>
> —Marcel Proust

IT project risks can be grouped into the three general categories of social, project management, and technical risks—or simply *People, Process,* and *Product* risks, respectively. Interestingly, the 17 EWSs with average ratings above a 6 (on our 7-point scale) belong only to the People and Process categories. This is not surprising since technology is almost never the root cause of IT project failure; although People and Process problems may manifest technically via inherent Product risks such as large size, high complexity, or novel technology. Nevertheless, these technical risks can be mitigated with proper People and Process practices, just like genetic propensities to certain diseases can be mitigated with proper behaviors, nutrition, and medications. Risks cannot be eliminated, but they can be managed.

It is worthwhile to consider that there are significant differences in the technical risks associated with make versus buy software acquisition strategies, as well as the degree of customization in the latter case and the degree of integration with existing sociotechnical environments in both cases. Nevertheless, since the most important EWS appear to be the non-technical ones, it is believed that the EWSs are basically the same across all these different technical situations. On the other hand, differences in technical risks do have important implications to the process and personnel dimensions of IT project risk and to the most effective risk mitigation approaches.

These 17 highest-rated risks were then distilled into the 12 most dangerous EWSs of IT project failure. These 12 EWSs can also be grouped into the four categories of the project's Stakeholders, Requirements, Management Processes, and Team. Table 1 shows these Deadly Dozen EWSs mapped to both the three risk categories and these Four Horseman of IT Project Doom. These various categorizations, distillations, and taxonomies of the top-rated EWSs are offered to provide auditors and other stakeholders with shortcuts

Table 1 *The Early Warning Signs of IT Project Failure*

The Deadly Dozen EWSS	The Four Horseman of IT Project Doom			
	Stakeholders	Requirements	Processes	Team
People-Related Risks				
1. Lack of top management support.	X			
2. Weak project manager.				X
3. No stakeholder involvement.	X			
4. Weak commitment of project team.				X
5. Team members lack requisite knowledge and/or skills.				X
6. Subject matter experts overscheduled.	X			
Process-Related Risks				
7. Lack of documented requirements and/or success criteria.		X		
8. No change control process or change management.			X	
9. Ineffective schedule planning and/or management.			X	
10. Communication breakdown among stakeholders.			X	
11. Resources assigned to higher priority project.		X		
12. No business case for the project.		X		

for remembering and observing material risks of IT project success. Nevertheless, these alone are but a starting point and may not provide the granularity or details necessary for properly auditing the EWS risks of a particular IT project with its particular requirements, personnel, processes, and organization.

What is interesting about the "Deadly Dozen" EWSs is that most relate to the governance, leadership, and management of IT investment activities. CFOs, CIOs, and CEOs should be deeply involved in leadership, governance, and risk management before and during the life of any significant IT investment. These EWSs are all important regardless of the technical profile of the project. The basic questions of What, Why, When, Who, Where, How, and How Much should be addressed in the IT governance and resource allocation processes before the investment is approved and funded, and those answers refined and monitored during the on-going monitoring, oversight, and management processes over the life of the project. While weak project teams are a highly rated EWS too, even a strong project team may not be able to overcome shortcomings in leadership and governance at the enterprise level. It is all too easy for senior management to be blind to the details and therefore risks of a particular IT project, even materially significant ones. Auditors, if they know what to look for, can be their eyes and ears to help obviate this tendency (Hettigei, 2004; Swanson, 2010).

The six people-related EWSs of IT project failure center on five not altogether mutually exclusive groups of People: top management, project management, project team members, subject matter experts (SMEs), and stakeholders in general. The six Process EWSs center on five project management processes and their associated deliverables that are essential to success: requirements (including a business case), change control, schedule, communications, and resources. In better-managed IT organizations all such process-related EWSs are typically combined into the official and repeatable IT development and project management methodologies, processes, methods, tools, and other practices applicable across the entire lifecycle of an IS. In best-practice situations, practices centered on many of the people-related risks are also incorporated into the

organization's official approach to IS development. The documents describing these processes and practices can provide the auditor, as well as the project manager and other stakeholders, with additional "check lists" for finding organization-specific EWSs.

IMPLICATIONS FOR AUDITORS

Risk management often involves significant judgment.
— John Mauldin

Successful management of IT projects is material to the accuracy of financial forecasts and regulatory reports, as well as for predicting enterprise capabilities in order to make viable plans and commitments. IT project success is critical to enterprise success, and to the career growth and success of CFOs, CIOs, CEOs, business unit executives, IT project managers, project team members, and even auditors. Failed IT projects not only damage organizations; they can also harm careers.

A Deadly Dozen risk indicators were found in the study to be the most important during the first 20% of an IT project's schedule. However, every project is unique, and so is every organization, so the relative importance of each EWS will be somewhat unique for every project. The three general risk categories, the "Deadly Dozen" and the "Four Horseman" of IT project risks do provide a valuable, quick, and easy starting point for seeing, monitoring, auditing, and managing the risks of an IT project. Nevertheless, it is advantageous in many situations to begin with the original list of 53 EWSs, or even an expanded more in-depth list of risks specific to a particular project's profile. Moreover, it is advisable to incorporate regular periodic audits into the organization's official processes of IS development and project management and that the frequency and depth of these depends on the overall risk profile and financial significance of a particular project.

Strategies for mitigating the risks indicated by a particular EWS are detailed in an earlier *EDPACS* article co-written by the author that also describes the research methodology and lists all 53 EWSs along with their rankings in the study and the sources in the literature from which they were derived (Kappelman et al., 2009). An alphabetical list of the 53 EWSs is provided in the Appendix of this article. Other valuable insights and recommendations are provided in Brooks (1986), DeMarco and Lister (2003), Gonzales (2008), Hay (2003), Hettigei (2004), Jones (2009), Nelson (2007), Singleton (2010), Swanson (2010), Yourdon (2003), and many other works not listed here. Providing definitive prescriptions for what auditors and other concerned parties must do when EWSs are found is beyond the scope of this article. Nevertheless, subtleties of organization politics aside, the abbreviated recommendation is simply to quickly make at least the project manager, CIO, and project sponsors aware of the risk, its significance, and its implications to the success of the project. Depending on the potential materiality of the project, the CEO, CFO, and board may also need to be promptly given notice.

Knowing about and paying attention to these EWSs—the earlier in the lifecycle of an IT project the better—increases the probability of a successful project outcome. Some IT projects should be stopped because circumstances have changed, it was a bad idea to start with, or it has become highly unlikely it will provide the promised business or financial benefits.

The critical role of auditors and EWSs in IT project success is much like the warning lights, gauges, and GPS (geographical positioning system) on the dashboard of an automobile. Seeing, paying attention to, and taking appropriate action regarding any warning signs from the beginning phases of an IT project can help avoid problems and help the enterprise and its leadership successfully reach their desired destination as safely and efficiently as possible.

References

The trouble is, if you don't risk anything, you risk even more.
—Erica Jong

Bernstein, P. L. (1996). *Against the Gods: The Remarkable Story of Risk*. New York: John Wiley& Sons.

Brooks, F. (1986). No silver bullet—Essence and accidents of software engineering. In H. Kugler (Ed.), *Information Processing 86* (pp. 1069–1076). Amsterdam: Elsevier; reprinted in F. P. Brooks, Jr. (1995), *The Mythical Man-Month, 20th Anniversary Edition*. New York: Addison-Wesley.

Carr, N. (2008). *The Big Switch: Rewiring the World, from Edison to Google*. New York: W. W. Norton.

Charette, R. N. (2005). Why software FAILS. *IEEE Spectrum* (September), 42–49.

DeMarco, T., & Lister, T. (2003). *Waltzing with Bears: Managing Risk on Software Projects*. New York: Dorset House.

Gonzales, S. (2008). SAS 70 reports—What do they really tell you? *Information Systems Control Journal,* ISACA. Retrieved December 20, 2010 from http://www.isaca.org/Journal/Past-Issues/2008/Volume-2/Documents/jopdf0802-sas-70-reports.pdf

Hay, D. C. (2003). *Requirements Analysis: From Business Views to Architecture*. New York: Prentice Hall.

Hettigei, N. T. (2005). The auditor's role in IT development projects. *Information Systems Control Journal*, v4. Retrieved November 29, 2010 from http://www.isaca.org/Journal/Past-Issues/2005/Volume-4/Documents/jpdf0504-The-Auditors-Role-in-develop.pdf

Jones, C. (2009). *Software Engineering Best Practices*. New York: McGraw Hill.

Kappelman L. A., R. McKeeman, & L. Zhang. (2009). Early warning signs of IT project failure: The dangerous dozen. *EDPACS* (*EDP Audit, Control, and Security*), *40*(6), 17–25.

Nelson, R. R. (2007). IT project management: Infamous failures, classic mistakes, and best practices. *MIS Quarterly Executive*, *6*(2), 57–78.

Singleton, T. W. (2010). The minimum IT controls to assess in a financial audit (part II). *ISACA Journal* (formerly *Information Systems Control Journal*). Retrieved December 20, 2010 from

http://www.isaca.org/Journal/Past-Issues/2010/Volume-2/Pages/The-Minimum-IT-Controls-to-Assess-in-a-Financial-Audit-Part-II-.aspx

Standish Group (2006). *The CHAOS Report*. West Yarmouth, MA.

Swanson, D. (2010). *SWANSON on Internal Auditing: Raising the Bar*. Cambridgeshire, UK: IT Governance Publishing.

Yourdon, E. (2003). *Death March: The Complete Software Developer's Guide to Surviving "Mission Impossible" Projects*, 2nd edition. New York: Prentice Hall.

Leon A. Kappelman, Ph.D., is a Professor of Information Systems, Director Emeritus of the IS Research Center, and a Fellow of the Texas Center for Digital Knowledge at the University of North Texas. He has helped many public and private organizations improve their IT management capabilities including American Heart Association; CIGNA; Coca-Cola; Executive Office of the President of the United States; Experian; HoneyBaked Ham; IBM; JCPenney; Kraft Foods; McDermott; Prudential; SAIC; State of Oklahoma; State of Texas; Treasury Department of Canada; United Nations; US Department of Veterans Affairs; Wells Fargo; World Bank; and others. He recently edited The SIM Guide to Enterprise Architecture (2010, CRC Press). For more about Dr. Kappelman visit http://courses.unt.edu/kappelman/.

An earlier version of this article written for CFOs and CIOs appeared as "Material Financial Risks of IT Projects: The Early Warning Signs of Failure" by Leon A. Kappelman, 2010, The Interpreter, a publication of the Insurance Accounting & Systems Association (IASA).

Special thanks and appreciation to my colleagues and co-authors on the original research: Robert McKeeman, MBA, PMP (Chairman, Utility Associates) and Lixuan Zhang, Ph.D. (Assistant Professor, School of Business and Economics, College of Charleston).

Appendix ***Alphabetical Listing of the 53 Early Warning Signs Used in the Study***

Approved project budget less than budget estimated by the project team
Budget, schedule scope and quality all mandated from outside the project team
Communication breakdown among project stakeholders
Cultural conflict among organizations involved.
Deliverable due dates missed during the first 10% of the project schedule
Difficulty in determining the input and output of the system
Early project delays are ignored—no revision to the overall project schedule
Earned value systems not in place or used to control program
Failure to gather requirement via Joint Application Design
Functional, performance, and reliability requirements and scope are not documented
IT operations infrastructure and network infrastructure problems have major impact on project team productivity
Key project stakeholders do not participate in major review meetings.
Key stakeholders do not review and signoff deliverables on a timely basis
Key stakeholders have not signed the Project Charter
Key team member turnover after project kickoff
Lack of top management support or commitment to the project
Large number of interfaces to other system required
Major new risks are identified after the project kickoff
No business case for the project
No change control process
No contingency budget for known risks and rate of changes
No documented analysis of business strategy alignment
No documented milestone deliverables and due dates

Appendix ***Continued***

No due diligence on vendor(s) and team members
No performance and reliability requirements metrics tracking process
No planning and estimation documentation
No Project Charter document at early stage of project
No project communications plan or resources devoted to managing and communicating project expectations
No Project Management methodology
No project status progress process
No risk analysis documentation and process
No team member experience with the chosen technology
No written commitment for the project outside of the project team
Project involves implementing a custom or beta version hardware or software
Project manager(s) cannot effectively lead the team and communicate with clients.
Project Manager(s) have never managed a project of this scale before
Project managers have poor training
Project resources have been assigned to a higher priority project
Project stakeholder decision delays have caused due dates to be missed
Project stakeholders have not been interviewed for project requirements
Project team member(s) have low morale
Project team members are overscheduled
Project team members do not have required knowledge / skills
Project team members have weak commitment to the project scope and schedule
Schedule deadline not reconciled to the project schedule
Significant goal, scope, or schedule requirements change immediately after project kickoff
Subject matter experts are overscheduled: retain all prior duties yet expected to provide substantial participation to the project
Team member have undefined roles and responsibilities
Undefined project success criteria
Unstable organization environment (such as changes in senior management or restructuring)
Users are not willing to cooperate
Users cannot get involved because lack of understanding of new system capabilities
Users or technical support team feels threatened by a project to replace their legacy system

Adapted from Kappelman, McKeeman, and Zhang (2009).