The two *overlooked* aspects of *IT risk* management

If a new IT system works well but doesn't increase user productivity or business results, who or what could be responsible? Usually, it's because someone forgot that IT risk isn't just about technical performance. IT projects have organizational and business risks that must be managed too

By Mike Campbell and Dutch Holland

Often, an IT department and its managers are criticized from above, when a new computing system they recently deployed fails to deliver promised business benefits. Sometimes when this happens, the IT group is baffled, because the system works exactly as advertised. They investigate further, and find that the reason users haven't become more productive is that they're using the new system incorrectly—or not using it at all.

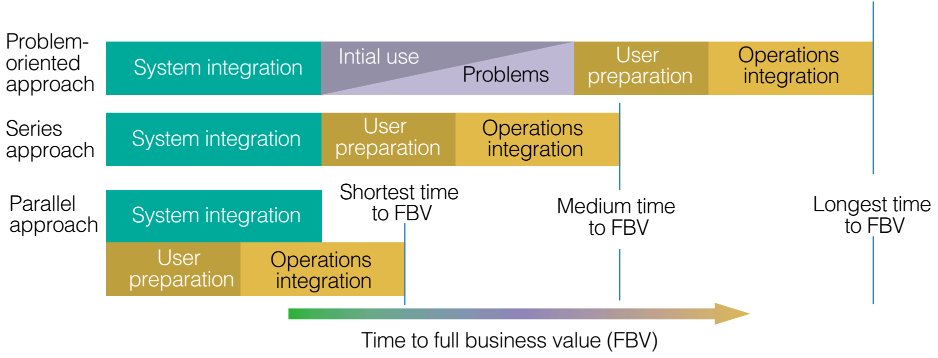
Whenever such a big piece of the puzzle is discovered missing after a system is deployed, a company's only recourse is to put the users through a crash training program. But it's not a real solution to the stalled productivity problem, because the delay in achieving expected benefits invalidates all the equations originally used to cost-justify the project. Ideally, the need for training should have been anticipated, and training should have been provided, before the new system went live.

If preparing users for a new system is so vital to the success of an IT project, one wonders why so many energy and other kinds of big companies fail to do it well or at all. Among the many reasons, the one to which companies most often admit is that they simply took the human aspect of technology use for granted, leaving user preparation up to user managers ill-prepared for the task. This is a lame excuse, because there is a discipline they could have used which eliminates such omissions in planning by making the planning process formal and rigorous. It is called change management, and initiating an industrial-strength, enterprise-wide version of a change management program is the only way to guarantee that a multi-million-dollar IT project indeed delivers its ROI payoff on time.

Big systems, big risks

While the benefits of big IT projects—like installing a new enterprise resource planning (ERP) or mapping system—have proved substantial to many companies, the implementation of such systems has proved to be a risky proposition. The size of the risk—which can extend beyond the tens of millions of dollars paid for the new sys-

Approaches to use of operations integration



tem to the hundreds of millions in potential disruption to the organization and its customers—calls for an aggressive and systematic risk management initiative to ensure success. That initiative must address the three kinds of risks associated with big systems implementation: technical risk, organizational risk, and business risk.

Coping with the three kinds of IT system risk

Manage	To ensure
Technical risk	The new IT system works technically
Organizational risk	Knowledge workers will use it correctly
Business risk	The benefits achieved are cost-justified

Most vendors and users of IT systems are familiar with management of technical risk. They measure how technically risky a system is by asking and answering the following pragmatic questions: Will the system work, will it work on time, and will it do so within budget? Usually, technical risk is managed reasonably well by a team of the user's and vendor's IT professionals.

Managing organizational and business risk

Successful, enterprise-wide deployments of big IT systems, however, require that two other kinds of risk also be measured and managed. One is organizational risk, a term that attempts to quantify the possibility that users won't exploit the full potential of the new system. Failure to do so could be caused by many factors; among the most common are inadequate user preparation and human resistance to change.

Business risk, by contrast, attempts to determine the odds that the new system will fail to deliver productivity and financial benefits that are worth more than the cost to achieve them. Here too, its failure to do so could be attributed to a number of factors. But one of the most common is a lack of alignment between the work processes embedded in the system and the company's business strategies and priorities.

Mitigating organizational and business risk

A change management initiative can be a powerful tool for mitigating organization and business risk—but only if it goes far enough. Too many such initiatives are too weak; by focusing only on publicizing the arrival of the new system, for example, they prepare users to accept the new system but do little to make them capable of using it. Stronger initiatives not only incorporate preparatory training, but also include elements designed to ensure that the new system is fully integrated into the day-to-day operations of all affected departments by the target date. Another way to characterize the objective of such an industrial-strength change management initiative is operations integration.

Operations integration comprises the body of knowledge and practices needed to be applied to ensure that a new system produces the desired results by a certain time at a specified cost. To succeed, its disciplined approach must be followed by all departments that will use the new system. Among its many required actions are:

- Clear communication of the corporate goals for the new system.
- Making it crystal-clear which workers will be expected to use it.
- Fine-tuning and aligning the company's work processes with the business processes embedded in the new system.
- Documenting the tuned and aligned processes in the company's official Policies and Work Procedures manual.
- Modifying workers' roles and job descriptions to account for the changes in the business processes and the workers' use of the new system.
- Training users to handle the work processes that use the new system.
- Creating incentives and disincentives for using the new system.

Move forward with operations integration

The bottom lines are simple:

- Operations integration must be done in order to mitigate organizational and business risks. As the chart on the previous page illustrates, the variations on when to begin can run the gamut from the problem-oriented approach, which takes the longest elapsed time, to the parallel approach, which takes the shortest time to full business value. Regardless of which option is chosen, senior management must demonstrate strong leadership and require that operations integration be done from the very start of the project.
- In addition, top management must require that the operations integration effort not be owned and led by the IT department, but by the highest ranking manager of the user groups that will be using the new system in their day-to-day business.
- IT leadership's role must be to ensure that top management fully understands that (1) IT will manage technical risk, and (2) only user management can properly mitigate organizational and business risk.

IT managers who do not insist that operations integration be properly owned and led run the very real risk that the IT system will not pay off for the company, and they will be blamed.

In summary, always keep in mind that risk cannot be avoided. It must be accepted and managed in any project that involves IT. But in managing risk, any project will have three risk components to manage successfully—technical, organizational, and business. ■

Mike Campbell is a managing director and Dutch Holland is CEO of Holland & Davis, a management consulting firm in Houston (www.hdinc.com). Dutch is the author of Red Zone Management: Changing the Rules for Pivotal Times.