

In 1995, the Standish Group began to publish reports of the IT failure rates of both public and private organizations in the United States. They suggested that more than 80 percent of systems development projects fail in whole or in part. Most projects cost more, take longer than planned, and fail to achieve all of their goals. One-third are canceled before they are completed.

One system development project cancellation took place at the State of California Department of Motor Vehicles (DMV) in the mid-1990s. The project to move nearly 70 million vehicle, license, and identification records from an antiquated system to a new relational database was both behind schedule and over budget.

When California's lawmakers finally decided to end the agency's IT project, over \$44 million had already been spent and no end was in sight. One of the reasons the DMV project failed, says California Assemblyman Phillip Isenberg, is "because the agency staff were over their heads with a technology they did not understand."

The project also lacked a clear link between agency operational goals and the capabilities of the selected technology. Due to procurement restrictions, the agency was committed to a specific hardware platform before all the available options could be explored. As a result of the failure, California's technology procurement process faces even greater control and oversight. Despite these problems, California has an annual IT budget of well over \$1 billion, and more big projects are on the horizon - as they are everywhere in the world.

In fact, government constitutes one of the world's largest consumers of information technology. Because of its size, complexity, and pervasive programs and services, government cannot operate effectively without using advanced information technologies. However, as the California DMV failure amply demonstrates, the risks of IT innovation in government are daunting.

Years of research on information system success and failure have been unable to conclusively identify the factors that cause good or bad results. Information technology success and failure seem to be in the eye of the beholder.

We've spoken to public managers who consider a project a success if it comes in on time and on budget. Others, who evaluate functionality and usability, might call the same project a failure. Many see failure when, regardless of time and budget, a new system makes it more difficult to do routine and familiar tasks. They have the latest technology but can't get their work done as well as they did before. We've heard about systems that perform beautifully, but can't be supported by in-house staff and therefore continue to generate high costs for consultants to maintain them.

Failure may be a desirable statewide system that local governments can't use because they lack their own expertise and technical infrastructure to connect to it. Failure has also been described as an on-time, on-budget system with great user interfaces and functionality, but users will not work with it because they don't trust the underlying data sources.

How do you protect against something you can't define? We advocate an approach that builds knowledge and understanding through careful analysis of the goals, the larger environment, the specific situation, the likely risks, and the reasonable alternatives. That kind of thinking will help you raise useful questions, engage partners, challenge old models, garner support, assess policies, identify risks, consider contingencies, and result in more successful innovation.

Risks of IT innovation

Expert observers of IT trends say organizations waste time, money, and credibility on IT because of a few fatal mistakes. They either buy the wrong technology for the job, or they buy the right technology but do not implement it effectively. They allow technical experts to design systems without the substantive, ongoing involvement of system users. They build systems that ignore the way people and processes really work. They don't take into account the other systems that are already in place. They start investing resources in an IT solution before they really understand their needs and options. They are overconfident that they will get it right and don't plan or budget for the inevitable post-implementation refinements that any system needs. They don't attend to environmental realities such as workforce limitations, election or business cycles, rapidly changing technologies, political processes, and competing priorities.

Clearly, IT innovation is risky business in every organization. Repeatedly, organizations abandon IT projects because these initiatives fail to accomplish the objectives they were intended to meet. In both the public and private sectors, a well-documented set of risks attends IT innovation.

Unrealistic expectations

Organizational perceptions of new technology are critical to achieving success. Positive expectations help lead to success, but too often overly optimistic expectations cause serious trouble. All the people involved in an IT initiative, from sponsors to users, need to have realistic goals and must share a common understanding of potential benefits, required policy and process changes, and the financial and organizational costs.

The technology is only a part, and often a small part, of the story. We've seen projects delayed or even halted due to unrealistic expectations about how quickly a project can be completed, about the human resource requirements, about how much collaboration was necessary and how costly it can be, and about how much and how many kinds of new learning and training would be required to build and use a new system.

Lack of organizational support and acceptance

Adoption of a new way of doing business or of a new technology is unlikely to succeed if it does not have widespread organizational support and acceptance. Much has been written about the critical importance of top management support and this is surely necessary. But, we've learned that success depends on many other organizational factors as well. It also takes skilled and committed team members and support and acceptance throughout the organization, especially among the people who will **use** the new processes and the new technology. Often this is the most important level of support, and often the most difficult to achieve.

Failure to evaluate and redesign business processes

IT management expert Michael Hammer says systems may not meet performance expectations because organizations "tend to use technology to mechanize old ways of doing business. They leave the existing processes intact and use computers simply to speed them up."

Meeting the needs of customers, employees, and decision makers means carefully studying and evaluating business processes. In most organizations, new processes are added as needed, but old processes are rarely evaluated to determine if they still make sense.

When new technology is brought into the picture, a cumbersome and inefficient process may be automated "as is." The results are systems that do not serve business needs, systems that are too expensive for the small productivity gains they provide, and systems that are not flexible enough to meet changing demands. This leads to poor performance in individual organizations and even worse problems when the system is expected to connect multiple programs or agencies, as is often the case in government.

In order to make system design work more manageable, we often ignore the ways in which one system affects related work processes. For example, an accounting system needs to factor in the ways in which accounting is related to budgeting, revenue collection, and financial management. The accounting function does not stand alone, and a system that supports accounting cannot behave as if it does.

Often organizations are not willing to invest the time and money necessary to do comprehensive process mapping and analysis. Many organizations see this as an unnecessary effort; in place of it they share procedures manuals (typically outdated and not reflective of what is going on) with system designers. Unfortunately, this sets up a "pay me now or pay me later" proposition. Ineffective or incorrect processes become embedded in the new system causing need for costly revisions or manual "work-arounds" that defeat the purpose of applying technology in the first place.

Lack of measurable alignment between organizational goals and project objectives

Another risk factor involves the alignment (or lack of alignment) between organizational and project objectives. The goal of IT adoption should be to enhance or improve an organization's ability to carry out its main mission or business objectives. For instance, it should improve customer service, reduce manual record keeping, speed up transactions, increase revenue, prevent errors, or support good and timely decisions. All of these kinds of improvements should be represented by baseline measures and target levels of performance. Without them, the technology tends to take on its own independent course, and fails to have its intended impact on how real people use information to accomplish real work.

Failure to understand the strengths and limitations of new technology

Information technology is constantly changing and improving. No one is able to keep up with the details of all new developments or to understand comprehensively how each new technical tool works. Add to this the fact that most new technologies must work in tandem with others, or must be incorporated into existing older systems, and the possibility for trouble mounts rapidly. Since most organizations are not in the IT evaluation business, they may rely on word of mouth, vendor claims, and trade publications for the bulk of their knowledge about which tools

may be right for which jobs. There is little opportunity to learn first-hand before making expensive, irrevocable decisions.

Projects that are too specialized or ambitious to manage successfully

For years, oversight organizations like the US General Accounting Office (GAO) have warned against information technology initiatives that some characterize as "grand designs." These are the projects whose scope is so large, time horizon so long, or design so unique that they will almost certainly falter or fail. Such projects invite delays, unexpected complications, gaps in funding, management nightmares, and other problems. Instead, most experts recommend that systems be designed and deployed in modules and be built on standard technologies using well-tested methodologies. This risk is relative and applies to large and small organizations. A town or county system with a price tag of \$15,000, in an overall budget of \$400,000, with an IT staff of one is just as ambitious as a multi-million dollar project in a large state or federal agency.

Public sector risks

Government seems to have even more trouble than the private sector in successfully applying new technology. The public policy choices and public management processes that are part of government make it an especially difficult environment for IT managers. Some contend that bid protests, relatively low government wages, and legislative interference lead large government information technology projects

This environment brings a layer of risks unique to the public sector. When added to the organizational, operational, and technical risks described above, they present a daunting challenge to public managers responsible for choosing, funding, and building IT innovations.

Limited authority to make decisions

By design, governmental authority is divided across multiple decision makers. Executive managers do not have a clear line of authority over operations. Their decisions are circumscribed by law, limited appropriations, civil service rules, and a variety of legally mandated procedures or court decisions. These restrictions do not blend well with the complexities of managing an expensive and complex IT project in a rapidly changing technical environment. Worse, as can be seen in the California DMV experience, when IT projects fail the common legislative response is to place more restrictions and more controls over the IT management process.

Multiple stakeholders and competing goals

Government programs are characterized by a multiplicity of stakeholders who often have competing goals. Customers, constituents, taxpayers, service providers, elected officials, professional staff, and others all have some stake in most programs. Some want more or different services, others want lower taxes or fewer rules. Understanding how different choices may affect each stakeholder group helps to identify likely conflicts and prevent unexpected problems.

One year budgets

Uncertainty about the size and availability of future resources weakens the ability of government agencies to successfully adopt new IT innovations. Most government budgets are handled on an annual cycle. While many agencies have developed planning mechanisms to cover a three to five year period, annual appropriations (influenced heavily by changing government-wide priorities) tend to negate long-term planning. As a result, funds promised for a project in the first year may not be continued during the second or subsequent years.

Highly regulated procurement

Most decisions to adopt emerging technologies are made through the traditional competitive bidding process. While the goals of competitive procurement are goals of integrity and fairness, the processes are often a source of problems and delays. Agencies write Requests for Proposals (RFPs) using the information they have been able to gain from limited research. Vendors spend large sums of money trying to develop the winning response. Time consuming, arms-length reviews and negotiations ensue. Losers often take advantage of bid protest procedures that can further delay contract awards for months-or even years. Due to insufficient project support or understanding by top management, IT procurement requests may receive low priority. The resulting delays can mean time and cost overruns which in turn yield negative publicity, decreased support from top management, and negative perceptions of the overall value of the effort. Commodity-based procurement, on the other hand, is easy for agencies to use, but assumes that they have all the information and expertise they need to design and

assemble a high- performance system out of a catalog of parts.

Little capability to design or operate integrated or government-wide programs

Critics (including many public officials themselves) complain that different government agencies operate more or less without regard to the fact that they often serve the same people. The difficult fact of life is that government is organized mostly into separate programs that receive specific authorization and funding from Congress or a state legislature. Accountability rules and traditions demand that these programs be operated separately, and one result is the famous "stovepipe" systems of government. Because these isolated programs emerge from deliberate design, they are very difficult to coordinate, much less integrate. New technologies, especially the Internet, are making it feasible to present a unified face to the public, but the changes that need to take place behind the scenes in policies, accountability mechanisms, processes, data sharing, and records management are only beginning to be understood.

Extreme risk aversion

Government's business is public business. This means that most new ideas have to be implemented in full public view. An innovation "gone wrong" risks not only dollars, but also the credibility of an agency and its leadership with legislators, executive officials, and the public. It's not surprising, then, that government tends to rely on the "tried and true."

How this guide can help

Government managers need to analyze and evaluate IT choices because these choices are among the most complex and expensive decisions they are expected to make. Whether you are a local official considering a new system to support building permits or an administrator at a large federal agency considering a new network infrastructure, you are faced with a complex and relatively expensive decision-making process. The consequences of your IT decisions often have a significant and direct impact on the public. For example, the safety of the flying public rests on the ability of the Federal Aviation Administration to implement systems that control air traffic. A state child welfare agency gathers and responds to information that protects the health and well being of children in that state. A local government emergency response application ensures that emergency vehicles are routed to incidents in the fastest and safest way possible. Systems that support law enforcement make a big difference in the ability of federal, state, and local criminal justice agencies to provide public safety. These systems cost thousands, millions, even billions of dollars. They are important because the goals they serve are crucial to our quality of life. The risks of system failure are linked to the risks of service failure for hundreds, thousands, or even millions of people.

This guide can't tell you what technology to buy, or even what problem is most important to solve. It can't tell you how much money you will save using IT, or even if you will save any money at all. This book is about how to **think about** an IT investment. It offers a set of analytical techniques to understand the issues and opportunities and to build a business case for investing in a particular path. It shows how to use that business case to get the support you need to move forward with your project. We think of this phase of the IT investment process as the one that comes "before the beginning." It is necessary before the first design meeting, before an RFP is written, before the budget is developed. We believe this kind of up front analysis is essential to doing all of those things well because it uncovers both risks and resources that lead to smarter IT decisions.

In short, three kinds of analysis mitigate the risks of these investments:

- thoroughly understand both the problem to be solved and its context
- identify and test possible solutions to the problem
- evaluate the results of those tests against clear service and performance goals

The following chapters present a well-tested methodology that can help you to understand and carry out these three critical tasks.

References

Hammer, Michael. (1990.) "Reengineering Work: Don't Automate, Obliterate," **Harvard Business Review**, July-August.

Isenberg, Phillip. (1994.) "Point of View: When BIG IT Projects Falter," **Government Technology**, July, 7(7).

Chapter 1. The risks of IT innovation in government

Miller, Brian. (1994.) "DMV Project Hits Dead End," **Government Technology**, July, 7 (7) pp. 1, 53-54. The Standish Group. (1995). **The CHAOS Report**. On line at

http://www.standishgroup.com/sample_research/chaos_1994_1.php