# CHAPTER 6

# Governance for a Redefined IT

IT is facing many new pressures to deliver faster, deliver different products and services, and work differently at all levels of the organization and with vendors, partners, and even customers. As a result, there is broad recognition that IT needs to redefine itself to be more effective for the future. Change is not optional for today's IT organizations. The major challenge for IT leaders is therefore deciding what to change and how fast to do it.

As this quote makes clear, the pressure is on IT to deliver faster and this means working differently. IT managers are in general agreement with this goal but also feel a responsibility to protect the organization and its data. Many of IT's so-called "bureaucratic processes" were put in place for good reasons, such as to ensure quality, interoperability, and cost-efficacy. And in many highly regulated industries, such as finance and health care, laws and risk-aversion govern much of what can and cannot be done by IT. Nevertheless, there is a need to reconcile these competing priorities and rethink how IT works.

IT work involves two major components: 1) making decisions about what work to do (i.e., strategy), and 2) delivering the work (i.e., execution). IT governance is the system of structures, processes, and roles that collectively *oversee* these two major components of IT work. Championing the needs of the enterprise (i.e., common processes, architecture, data, and controls) favors more centralized forms of governance just as championing responsiveness to the business favors more decentralized (or perhaps hybrid) forms of governance. Balancing these is at the nub of the challenge for today's IT leaders: the need to act faster and in closer alignment with the business while still protecting the organization's overarching interests.

## The Increasing Importance of Governance

IT governance is a framework of processes and structures that specify who makes decisions about and who is accountable for the IT function and its work. It also determines who should have input to issues, how disputes should be settled, and how decisions should be made, implemented, and managed (Weill and Ross 2005). It is *not* about what specific decisions are made or how groups are organized and led. Effective IT governance is designed to encourage desirable behavior in the use of IT that is consistent with an organization's mission, strategy, and culture (Weill 2004).

Research shows that effective governance has a significant influence on the benefits an organization receives from its IT investments. Value is achieved by ensuring "that the right groups are making the key IT decisions so that those decisions enable the desired goals and behaviors of the enterprise" (Weill 2004). Although it does not point to a single best governance model, effective governance is carefully designed to link to an organization's particular performance goals (Weill and Ross 2005).

A significant reason for an organization's ability to derive value from IT is that its governance provides senior leaders with a clear understanding of how IT decisions are made, thus helping to: 1) clarify business strategies and IT's role in achieving them, 2) measure and manage IT investments, 3) design organizational

practices to align IT and business strategies, 4) assign accountability for change, and 5) learn (Weill 2004). Therefore, it is unfortunate that IT governance has all too often been found to be a mystery to key decision-makers at most companies (Weill and Ross 2005).

Although getting value from IT is an important reason for leaders to design for effective governance, in recent years a number of other factors have also become drivers for senior managers to focus on it. These include:

- ***Ensuring privacy and security.*** Concerns about security have now reached the board level. More and more, CIOs are being asked to present their IT security plans to directors, who recognize that a security breach could at minimum embarrass their company, and potentially cause significant losses. Recent accounts of major customer information losses due to security lapses have heightened attention to the need to have effective governance of security practices even in the most insignificant areas.
- ***Compliance with laws and regulations.*** There was general agreement in the focus group that there is a growing amount of legislation affecting governance, that regulators in specific industries are becoming more demanding, and that both internal and external auditors are becoming more intrusive and prescriptive in their reports. "This all results in more process and additional work," said a manager. While not all industries are regulated, many are. In this focus group, companies from the finance, insurance, healthcare, travel, and food industries all noted the increasingly onerous burden of regulation. And all companies are feeling the pressure of new legislation and more detailed audits. In addition, international or global companies must comply with a variety of individual country regulations, such as separating data or management oversight.
- ***Improving risk management.*** IT work has become more complex and is less often under direct management control. Today's IT service offerings typically include third-party software developed by outsourced staff (often not even in the same country) and rely on a rapidly evolving ecosystem of service providers in emerging industries (e.g., cloud, software-as-a-service). Under these circumstances, it is all the more important for governance to recognize and address the additional vulnerabilities involved.
- ***Improving alignment between strategy and execution.*** Often organizations have misaligned governance structures—one for innovation and strategic projects and another for execution and operations. If actions in one ignore governance requirements in the other, such as when putting new changes into operational systems or circumventing existing architecture, then governance is undermined to the detriment of the company as a whole.
- ***Increasing customer involvement.*** As technology touches the lives of end customers more often and is more visible, corporate reputations are increasingly at risk. As one manager put it: "It's important that we use customer information to interact with our customers appropriately or it could be embarrassing or worse."

Group members commented that with so many competing dynamics, it is especially difficult to design governance without adding significant extra work for IT staff. "Our goal is to design governance that is *enabling,"* said a member. "If everyone understands their roles and responsibilities, when they need permission, and the right people have the right tools, then this is possible. Not everyone will like it but at least it is clear." Another added, "Our goal is to make effective governance a part of our culture. We want to build integrity into everything we do."

It is clear that governance is more of a challenge the larger a company gets, and it's a greater challenge in some industries or countries than in others. Regardless of the company, the need for effective IT governance has

never been more evident, and companies are scrambling to keep up as IT itself changes and the interaction between these drivers evolves.

## Elements of Effective IT Governance

Effective governance is not attained by a single committee or set of rules, except perhaps in very small organizations. Instead, it is achieved through an integrated framework of organizational groups that provide oversight in different areas, standards, and practices founded on industry best practices, legal and compliance requirements, and policy guidelines that direct how work is to be accomplished. Governance should be designed to provide clarity and consistency to IT work and focus IT decisions on what is most important to the organization. It should also ensure that governance practices support each other, rather than work at cross-purposes.

A governance framework most often operates at three levels, although this may vary according to size and geographic needs:

- ***Board governance.*** While board level governance involves more than IT, boards are increasingly aware of their responsibility to become better informed about the IT decisions made in their organizations. Boards are responsible to their shareholders for managing both the finances of their companies and the risks they undertake, as well as their reputation and brands. In addition, a board is responsible for ensuring that its organization is compliant with all regulatory requirements and reporting, and for addressing all issues raised by its internal and external auditors. Each of these can now be significantly affected by IT strategy and execution. One need only pick up a newspaper these days to see how damaging it is for a board to fail in its oversight of one or more of these areas. Thus many boards now have technology committees or at least members who have some technology background, and IT matters are being more frequently questioned at this level. This is a positive change according to the focus group, as it raises the profile of serious IT concerns to the highest echelons in the firm.
- ***Enterprise IT governance.*** This is a level of governance that is growing considerably as IT leaders realize the value that good governance can deliver. As Figure 6.1 shows, enterprise IT governance provides detailed integration of factors affecting IT decision-making in several areas including:

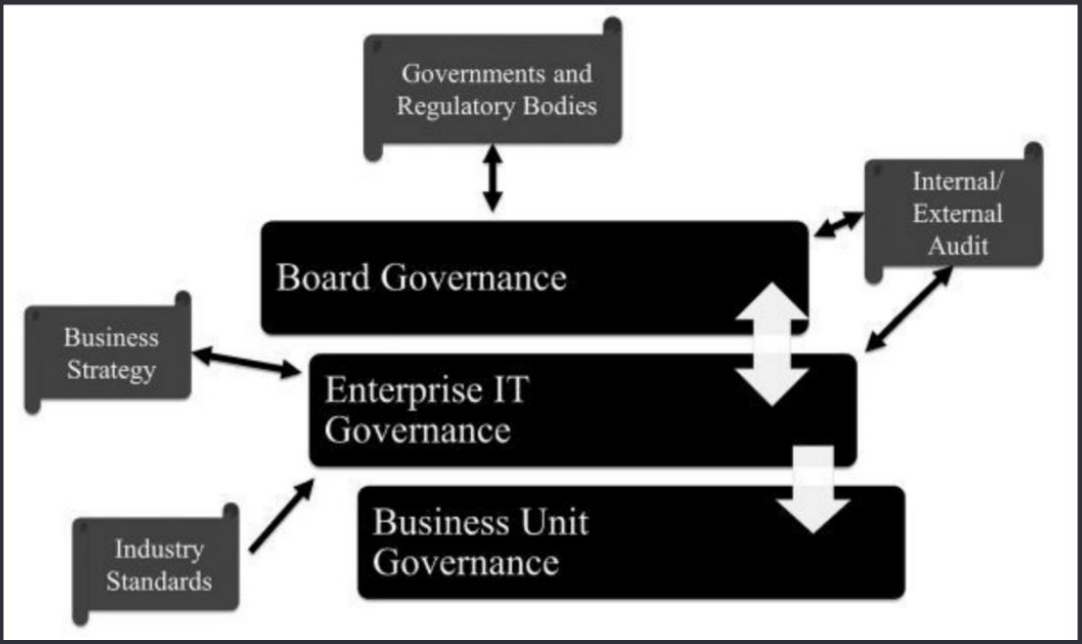


**Figure 6.1** IT governance integrates many components.

*Architecture.* This sets current and future technology strategy, ensuring it is consistent with overall business strategy. It identifies best practices and industry standards for use in IT and provides oversight and approvals for all technology initiatives to ensure that the company is both protected and positioned well for the future.

*Security and privacy.* This provides oversight and guidance on all security matters to ensure that the organization's information assets and infrastructure are protected and to proactively and continuously address security risks. It also oversees access management practices.

*Operations.* This ensures that all technology implementations and changes follow proper procedures and standards, and provides oversight of all ongoing operations. It also reviews and reports on ongoing service levels and seeks to ensure that risks are mitigated and issues resolved.

*Strategic projects.* This oversees the processes designed to ensure that the most strategically valuable projects are properly and expeditiously resourced and funded. It also tracks project progress to ensure that all standards are followed and risks identified and mitigated.

*IT capabilities.* This ensures that IT has the necessary capabilities to carry out its mandate, whether internal or external, and also oversees the organization's relationship with its vendors and service providers, ensuring they meet all standards and contractual responsibilities.

*Data.* This is the newest component of IT governance, responsible for managing data as a strategic asset, building a common framework and definitions for key corporate data, and developing effective data management practices and accountabilities.

- ***Local (business unit) governance.*** Most organizational governance frameworks also allow for some discretionary IT decision-making. This involves making decisions about smaller-scale, lower-cost, new applications and prioritizing changes to existing IT applications to be made in the business units. In general, organizations try to limit business unit IT decisions in order to focus the vast majority of IT spending on

higher-value, strategic initiatives. And most recognize the need for this level of decision-making to support local flexibility. Enterprise IT provides oversight for and input to this level of governance, ensuring it follows appropriate practices and standards for development, testing, and implementation.

## IT Governance Evolution

Once designed, IT governance should not need to be rethought simply because of changes in the economy or adjustments to strategy (Weill 2004). Circumstances under which governance should be completely reevaluated include a major change in strategy or a merger. Within these two extremes, however, lies the area of "practical governance," which involves enhancing, extending, or tweaking governance models to provide more clarity or to adapt to changing IT practices. "We have evolved our current governance model over the past six or seven years," said one manager, "and we still have areas that we need to address more fully."

- ***Third party vendors/outsourcers.*** Many companies have found gaps in governance and assumptions about decision-making when work is subcontracted out to third parties, who may in turn subcontract out some work. This can lead to any number of problems from a legal, audit, compliance, security, or privacy perspective. For example, "We thought we could outsource application development to get it done more quickly, but then we found we had to retrofit these applications to meet our security criteria. This was very painful," said a manager. "Because IT still has accountability for products developed in this way, we've found it necessary to add extra layers of due diligence when dealing with third parties," said another. Although it introduces additional complexity, there was general agreement in the group that with a good governance framework in place, and if vendors understand it well, shifting IT work to third parties can be successful.
- ***Cloud services providers.*** "With cloud software-as-a-service, we at first naively assumed we could impose our own controls, but with these large cloud vendors, *you* have to adapt," said one manager. Under these circumstances, companies must be extra vigilant to ensure that cloud vendors meet all corporate, regulatory, and government criteria, such as where data is located. Many countries explicitly prohibit their data from virtually or physically leaving their borders. In these cases, companies must evaluate their own processes and policies as well as those of their vendors to both adjust their internal governance practices and ensure that certain minimum standards are adhered to by their provider. "If these can't be met, you shouldn't be doing business with them," said a manager.
- ***Mobility and other new technologies.*** Although new technologies do not affect governance per se, there are at least three reasons why governance needs to be reconsidered when they are introduced. First, the technologies themselves may contain new vulnerabilities that have never been considered. For example, company tablets may contain confidential information or customer data that could be stolen or hacked due to immature protections on these devices. Second, in the rush to implement new technology and innovative applications, a company may be pressured to short circuit tried-and-true practices that could cause anything from operational issues to simple malfunctions to occur. Many companies are experimenting with new technologies these days and so developing ways to explore potential opportunities safely without circumventing existing governance practices is a challenge for IT leaders. One company in the focus group has a "fast track" approval process that enables strategically desirable projects to jump the queue in the prioritization process, while still following the standard review procedures afterward; another has developed a "governance-lite" approach for pilots, with the understanding that if the decision is made to

scale these up into production, they will follow all proper procedures. Third, new technologies typically have immature and rapidly changing standards that make it difficult to integrate into a technical architecture. An IT nightmare can occur if different projects select similar new technology that operates in different ways. Good governance prevents this from occurring.

- ***Data.*** The most challenging area of governance at present for many companies is data, and it is often a political hot potato. "Data has been a very painful journey," sighed one manager. "We've tried to do it many times before. We're now confident we have the commitment and the roles, responsibilities, accountabilities, and processes clear, but we are still meeting bi-weekly to figure out what's not working and who's not engaged so that we can deal with it. Otherwise, we'd be wasting our time." Good data governance requires consistent standards for each piece of data, but without clarity about who owns what, who produces it and who uses it, the information produced can be inaccurate or conflicting. One company learned a hard lesson when its CFO asked for integrated revenue data only to learn that different business units had different mechanisms for calculating this figure, which made the information highly suspect. "We needed to start top down and determine who owned which data and who had a mandate for changing it," said the manager involved. "We had a good data architecture for sourcing data but needed governance. We are now looking to develop data standards and good management practices."

In these new areas, governance best practices are not yet mature, and companies are trying to adapt their existing governance models to fit the need. Managers in the focus group stressed the importance of monitoring new governance practices as they evolve to ensure they are working well and doing what they are supposed to do. Without this attention, governance models can fall into disuse or become so bureaucratic that a company is seriously impeded in its work. "Good governance should help everyone understand the rules and make sure that the right levels have the right tools and responsibilities. We should never lose sight of this when designing governance," said a manager.

## Promoting Effective IT Governance

Focus group members had several recommendations for managers seeking to re-design or improve their IT governance practices:

1. ***Make fact-based decisions.*** "Ideally, all decisions should be based on facts, not gut feel," said a manager. "But we still have some way to go in this area." The group agreed that the more facts that are brought to bear on a decision, the better that decision will be. Facts improve clarity and consistency and create trust in the decisions that are made. As a result, they also encourage people to play by the rules and reduce "politicking."
2. **Work *from the premise that one size does not fit all.*** Governance in any company should be as simple as possible with a limited number of goals (Weill 2004). However, the group emphasized that governance will vary according to the industry, size of company, and geographical makeup of the organization. Thus a global financial company will need a more complex governance model than a small firm in a less-regulated industry. Many companies have been successful with different governance models (Wade and Buttchel 2013). "Small companies and large ones have the same set of issues, but they need to deal with them differently," said one manager. Similarly, centralization is not necessarily better than decentralization. "We should aim for the right model for the right types of decisions," said a manager. "We shouldn't centralize simply for the sake of centralizing," added another.

3. ***Monitor and iterate.*** Although governance models should be carefully designed to reinforce an organization's goals, they are not easy to get correct the first time. The group stressed the importance of monitoring how a model works in practice and making adjustments to ensure all processes integrate smoothly and efficiently. "It is especially important to align strategy and execution governance," said a manager. There can also be resistance to governance that is perceived to be inhibiting. The group stressed understanding where governance is not working and why, adapting it in some cases and reinforcing the rules in others. "At some point, you have to say 'these are the rules' but you also need to make sure that the culture is aligned top-down to meet these goals or governance will be perceived as intolerably bureaucratic," a manager commented.

4. ***Communicate from the top.*** It is essential that the CIO and senior leadership team communicate strategy clearly throughout the organization and educate all levels of personnel about the rationale for key governance mechanisms. Ideally, governance should be able to be communicated on a single page and education should be used to better align the culture with organizational objectives. "Often we see that our VPs are aligned with our goals but this doesn't filter down to other levels where our projects are actually implemented. We therefore need a much heavier focus on communication and education to reinforce governance," said a manager.

5. ***Clarify strategies and principles for staff augmentation.*** With so much IT work now being done by vendors, it is critically important to ensure that an organization has clear strategies and principles for how staff augmentation is to be handled. Organizations need to ensure that vendors comply with their governance practices and that staff is fully trained in what is expected. According to one manager: "This is especially important when dealing with offshore companies who may have different assumptions from our own. We've learned that we have to select vendors very carefully and hold them to very high standards. In our company, we rigorously review all outsourced work to ensure staff has followed our practices."

6. ***Include release valves.*** Even the best designed governance model needs an exception process to handle justifiable deviations from best practices, said the group. "Standards are black and white," said a manager. "We need to have ways to exempt projects from them if there's a good reason, such as a compelling business opportunity." However, exemptions should only be made after a clear consideration of the potential impact and risks, and often for a limited time period. This might be the case if a project wants to use a new and untried technology or if a competitor has come out with a new product or service that has rapidly become "table stakes."

## Conclusion

Effective IT governance is an essential element of delivering IT value. Designed well, it can facilitate alignment with corporate strategy and performance objectives and enable best practices in risk management, security and privacy protection, audit-ability, and information management. It ensures that the right decisions are made by the right people at the right time and provides guidelines for how best to address redefining IT. Designed poorly, it can be a roadblock to innovation, hinder performance, encourage non-compliance with the rules, and wrap the organization up in red tape. CIOs play a very clear role in setting the right tone at the top, promoting education about the role of governance, and creating transparent processes based on facts. There are many excellent governance guidelines available for IT leaders to use as a starting point, but they must also make the time to ensure that their governance actually works in practice and make adjustments where needed.

# CHAPTER 7

# The IT Budgeting Process

Forget about trying to contact an IT manager in September because you won't get very far. September is budget month for most companies, and that means that most managers are hunkered down over a spreadsheet or in all-day meetings trying to "make the numbers work." "Budgeting is a very negative process at our firm," one IT manager told us. "And it takes way too long." Asking many IT managers about budgeting elicits much caustic comment. Apparently, significant difficulties with IT budgeting lead to widespread disenchantment among IT leaders, who feel much of the work involved is both artificial and overly time-consuming.

Others agree. While there has been little research done on IT budgeting per se (Hu and Quan 2006; Kobelsky et al. 2006), there appears to be broad, general consensus that the budgeting processes of many corporations are broken and need to be fixed (Buytendijk 2004; Hope and Fraser 2003; Jensen 2001). There are many problems. First, budgeting takes too long and consumes too much managerial time. One study found that budgeting is a protracted process taking at least four months and consuming about 30 percent of management's time (Hope and Fraser 2003). Second, most budgeting processes are no longer effective or efficient. They have become slow and expensive and disconnected from business objectives (Buytendijk 2004). Third, rigid adherence to these annual plans has been found to stifle innovation and discourage frontline staff from taking responsibility for performance (Hope and Fraser 2003; Norton 2006). And fourth, although many researchers have studied how organizations choose among strategic investment opportunities, studies show that the budgeting process frequently undercuts management's strategic intentions, causing significant frustration among managers at all levels (Norton 2006; Steele and Albright 2004).

Finally, the annual planning cycle can cast spending plans "in concrete" at a time when the business needs to be flexible and agile. This is particularly true in IT. "Over time ... IT budgeting processes become institutionalized. As a result, IT investments become less about creating competitive advantages for firms [and] more about following organizational routine and creating legitimacy for management as well as organizations" (Hu and Quan 2006). Now that senior business leaders recognize the strategic importance of IT and IT has become many firms' largest capital expenditure (Koch 2006), a hard look at how IT budgets are created is clearly merited.

In this chapter we first look at key concepts in IT budgeting to establish what they mean for IT managers and how they can differ among IT organizations. Then we explore why budgets are an important part of the management process. Next we examine the elements of the IT budget cycle. Lastly, we identify some recommended practices for improving IT budgeting.

## Key Concepts in IT Budgeting

Before looking at how budgeting is actually practiced in IT organizations, it is important to understand what a budget is and why an effective IT budgeting process is so important, both within IT and for the enterprise as a whole. Current organizational budgeting practices emerged in the 1920s as a tool for managing costs and cash flows. Present-day annual fixed plans and budgets were established in the 1970s to drive performance improvements (Hope and Fraser 2003). Since then, most organizations have adhered rigidly to the ideals of

this process, in spite of much evidence of their negative influence on innovation and flexibility (Hope and Fraser 2003). These problems are clearly illustrated by the impact this larger corporate fiscal management process has on IT budgeting and the problems IT managers experience in trying to make their budget processes work effectively. The concepts and practices of the corporate fiscal world bear little similarity to how IT actually works. As a result, there are clear discontinuities between these two worlds.

These gaps are especially apparent in the differences between the fiscal view of IT and the functional one. *Fiscal IT budgets* (i.e., those prepared for the CFO) are broken down into two major categories: *capital expenditures* and *operating expenses*, although what expenditures go into each is highly variable across firms. In accounting, capital budgets are utilized to spread large expenses (e.g., buying a building) over several years, and operating expenses cover the annual cost of running the business. The distinction between these two concepts gets very fuzzy, however, when it comes to IT.

Generally speaking, all IT organizations want to capitalize as much of their spending as possible because it makes their annual costs look smaller. However, CIOs are limited by both organizational and tax policies as to the types of IT expenditures they can capitalize. It is the CFO who, through corporate financial strategy, establishes what may be capitalized, and this, in turn, determines what IT can capitalize in its fiscal budget and what it must consider as an operating expense. As a result, some firms capitalize project development, infrastructure, consulting fees, some cloud computing costs, and full-time staff, whereas others capitalize only major technology purchases.

How capital budgets are determined and the degree to which they are scrutinized also vary widely. Some firms allocate and prioritize IT capital expenses out of a corporate "pot"; others manage IT capital separately. Typically, capital expenses appear to be more carefully scrutinized than operating expenses, but not always. It is surprising to learn how different types of expenses are handled by different firms and the wide degree of latitude allowed for IT costs under generally accepted accounting principles. In fact, there are few generally accepted accounting principles when it comes to IT spending (Koch 2006). As a result, researchers should use caution in relying on measures of the amount of capital spent on IT in firms or industries.

It is within this rather fuzzy fiscal context that the structure and purpose *of functional IT budgets* (i.e., those used by IT managers as spending plans) must be understood because these accounting concepts do not usually correspond exactly with how IT managers view IT work and how they plan and budget for it. In contrast to how fiscal IT budgets are designed, IT managers plan their spending using two somewhat different categories: *operations costs* and *strategic investments*.

- ***Operations costs.*** This category consists of what it costs to "keep the lights on" in IT. These are the expenses involved in running IT like a utility. Operations involves the cost of maintenance, computing and peripheral functions (e.g., storage, network), and support, regardless of how it is delivered (i.e., in-house or outsourced). This category can therefore include both operating and capital costs. Between 50 and 90 percent of a firm's IT budget (average of 76 percent) is spent in this area, so the spending involved is significant (Gruman 2006). In most firms there is continual pressure on the CIO to reduce operations costs year after year (Smith and McKeen 2006).
- ***Strategic investments.*** The balance of the IT budget consists of the "new" spending—that is, spending on initiatives and technology designed to deliver new business value and achieve the enterprise's strategic objectives. Because of the interactive nature of IT and business strategy, this part of the IT budget can include a number of different types of spending, such as business improvement initiatives to streamline

processes and cut costs, business-enabling initiatives to extend or transform how a company does business, business opportunity projects to test the viability of new concepts or technologies and scale them up, and sometimes be considered capital expenses whereas others are classified as operating expenses.

Another fuzzy fiscal budgeting concept is *cost allocation—the* process of allocating the cost of the services IT provides to others' budgets. The cost of IT can be viewed as a corporate expense, a business unit expense, or a combination of both, and the way in which IT costs are allocated can have a significant impact on what is spent for IT. For example, a majority of companies allocate their IT operating expenses to their business units' operating budgets—usually using a formula based on factors such as the size and previous year's spending of the business unit. Similarly, strategic expenses are typically allocated on the basis of which business unit will benefit from the investment. In today's IT environment, these approaches are not always effective for a number of reasons.

Many strategic IT investments involve the participation of more than one business unit, but budgeting systems still tend to be designed around the structure of the organization (Norton 2006). This leads to considerable artificiality in allocating development resources to projects, which in turn can lead to dysfunctional behavior, such as lobbying, games, nonsupportive cross-functional work, and the inability to successfully implement strategy (Buytendijk 2004; Norton 2006). "We don't fund corporate projects very well," admitted one manager whose company allocates all costs to individual business units.

Allocations can also lead to operational inefficiencies. "The different allocation models tend to lead to 'gaming' between our business units," said another participant. "Our business unit managers have no control over their percentage of operating costs," explained a third. "This is very frustrating for them and tends to be a real problem for some of our smaller units." Because of these allocations, some business units may not be willing to share in the cost of new hardware, software, or processes that would lead to reduced enterprise costs in the longer term. This is one of the primary reasons so many IT organizations end up supporting several different applications all doing the same thing. Furthermore, sometimes, when senior managers get disgruntled with their IT expenses, this method of allocating operations costs can lead to their cutting their IT operational spending in ways that have little to do with running a cost-effective IT organization. For example, one company cut back on its budget for hardware and software upgrades, which meant that a significant percentage of IT staff then had to be redeployed to testing, modifying, and maintaining new systems so they would run on the old machines. Although IT managers have done some work educating their CEOs and CFOs about what constitutes effective cost cutting (e.g., appropriate sourcing, adjusting service levels), the fact remains that most business executives still do not understand or appreciate the factors that contribute to the overall cost of IT. As a result, allocations can lead to a great deal of angst for IT managers at budget time as they try to justify each expense while business managers try to "nickel and dime" each expense category (Koch 2006).

As a result of all this fuzziness, modern IT budgeting practices do little to give business leaders confidence that IT spending is both effective and efficient (Gruman 2006). And the challenges IT managers face in making IT spending fit into contemporary corporate budgeting practices are significant.

## The Importance of Budgets

Ideally, budgets are a key component of corporate performance management. "If done well, a budget is the operational translation of an enterprise's strategy into costs and planned revenue" (Buytendijk 2004). Budgets are also a subset of good governance processes in that they enable management to understand and communicate

what is being spent and where. Ideally, therefore, a budget is more than a math exercise; it is "a blueprint for fiscally sound IT and business success" (Overby 2004). Effective IT budgeting is important for many reasons, but two of the most important are as follows:

1. ***Fiscal discipline.*** As overall IT spending has been rising, senior business leaders have been paying much closer attention to what IT costs and how its budgets are spent. In many organizations a great deal of skepticism remains that IT budgets are used wisely, so reducing spending, or at least the operations portion of the budget, is now considered a key way for a CIO to build trust with the executive team (Gruman 2006). Demonstrating an understanding and appreciation of the realities of business finance has become a significant part of IT leadership (Goldberg 2004), and the ability to create and monitor a budget is therefore "table stakes" for a CIO (Overby 2004).

   It is clear that senior executives are using the budgeting process to enforce tougher rules on how IT dollars are spent. Some organizations have centralized IT budgeting in an effort to better understand what is being spent; others are making the link between reducing operations spending and increasing investment in IT a reason for introducing new operations disciplines (e.g., limiting maintenance, establishing appropriate support levels). Still others have established tighter requirements for business cases and for monitoring returns on investment. Organizations also use their IT budgets to manage and limit demand. "Our IT budget is capped by our CEO," stated one manager. "And it's always less than the demand." Using budgets in this way, although likely effective for the enterprise, can cause problems for CIOs in that they must in turn enforce spending disciplines on business unit leaders.

   Finally, budgets and performance against budgets are key ways of holding IT management accountable for what it spends, both internally to the leadership of the organization and externally to shareholders and regulatory bodies. Improperly used, budgets can distort reality and encourage inappropriate behavior (Hope and Fraser 2003; Jensen 2001). When used responsibly they can be "a basis for clear understanding between organizational levels and can help executives maintain control over divisions and the business" (Hope and Fraser 2003). Research is beginning to show a positive relationship between good IT budgeting practices (i.e., using IT budgets to manage demand, make investment decisions, and govern IT) and overall company performance (Kobelsky et al. 2006; Overby 2004).

2. ***Strategy implementation.*** Budgets are also the means to implement IT strategy, linking the long-term goals of the organization and short-term goal execution through the allocation of resources to activities. Unfortunately, research shows that the majority of organizations do not link their strategies to their budgets, which is why so many have difficulty making strategic changes (Norton 2006). This is particularly true in IT. As one manager complained, "No one knows what we're doing in the future. Therefore, our goals change regularly and at random." Another noted, "The lines of business pay little attention to IT resources when they're establishing their strategic plans. They just expect IT to make it happen."

   Budgets can affect IT strategy implementation in a number of ways. First, *where* IT dollars are spent determines the impact IT can have on corporate performance. Clearly, if 80 percent of IT expenditures is going to operations and maintenance, IT can have less strategic impact than if this percentage is lower. Second, how discretionary IT dollars are spent is important. For example, some companies decide to invest in infrastructure and others do not; some will choose to "bet the company" on a single, large IT initiative, and others will choose more focused projects. In short, the outcome of how a company chooses among investment opportunities is reflected in its budgets (Steele and Albright 2004).

Third, the budgeting process itself reflects and reinforces the ability of strategic decision-making to have an impact. Norton (2006) states that because budget processes are inherently biased toward the short term, operational needs will systematically preempt strategic ones. In IT the common practice of routinely allocating a fixed percentage of the IT strategic budget to individual business units makes it almost impossible to easily reallocate resources to higher-priority projects at the enterprise level or in other business units. In addition, siloed budgeting processes make it difficult to manage the cross-business costs of strategic IT decisions.

Overall, budgets are a critical element of most managerial decisions and processes and are used to accomplish a number of different purposes in IT: compliance, fiscal accountability, cost reduction, business unit and enterprise strategy implementation, internal customer service, delivering business value, and operational excellence, to name just a few. This, in a nutshell, is the reason IT budgeting is such a complex and challenging process.

## The IT Planning and Budget Process

Given that IT budgets are used in so many different ways and serve so many stakeholders, it is no wonder that the whole process of IT budgeting is "painful," "artificial," and in need of some serious improvement. Figure illustrates a generic and simplified IT planning and budgeting process. This section outlines the steps involved in putting together an IT budget utilizing some of the key concepts presented earlier.

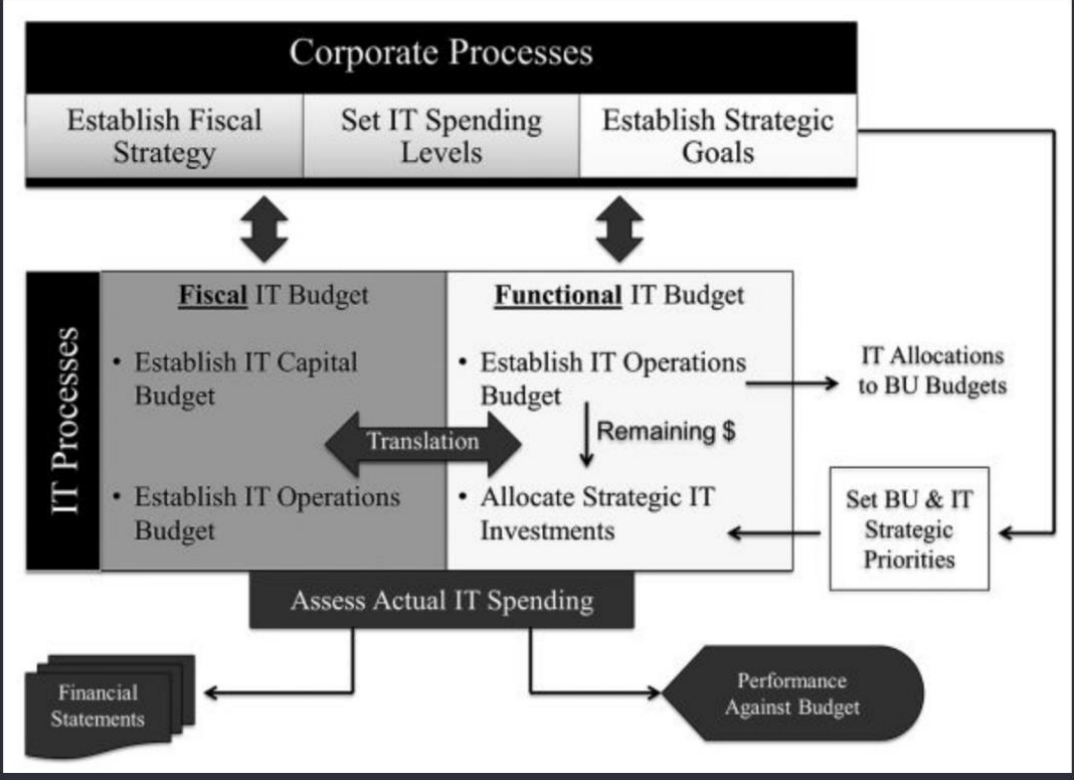


**Figure 7.1** A generic IT planning and budgeting process

### Corporate Processes

The following three activities set the corporate context within which IT plans and budgets are created.

1. ***Establish corporate fiscal policy.*** This process is usually so far removed from the annual budget cycle that IT leaders may not even be aware of its influence or the wide number of options in the choices that are made (particularly around capitalization). Corporate fiscal policies are not created with IT spending in mind but, as noted above, can significantly impact how a fiscal IT budget is created and the levels of scrutiny under which certain kinds of expenses are placed. A more direct way that corporate fiscal policies affect IT is in company expectations around the return on investment for IT projects. Most companies now have an explicit expected return rate for all new projects that is closely monitored.

2. ***Establish strategic goals.*** Conversely, IT budgeting is directly and continuously affected by many corporate strategic goals. The process of establishing IT and business unit strategies occurs within the context of these overall goals. In some organizations there is tight integration between enterprise, business unit, and IT strategic planning; in others these elements are more loosely coupled, informal, and iterative. What is truly rare is a provision for enterprise funding for enterprise IT initiatives. Rather, corporate strategic goals are typically broken down into business unit budgets. As one manager explained, "First our executives decide our profits and then the business units decide how to achieve them, and then IT develops a plan with the business unit.... We still don't do many corporate projects."

3. ***Set IT spending levels.*** Establishing how much to spend on IT is the area that has been most closely studied by researchers. This is a complex process, influenced by many external and internal factors. Externally, firms look to others in their industry to determine the level of their spending (Hu and Quan 2006). In particular, companies frequently use benchmarks with similar firms to identify a percentage of revenue to spend on IT (Koch 2006). Unfortunately, this approach can be dangerous for a number of reasons. First, it can be a strong driver in inhibiting competitive advantage and leading to greater similarities among firms in an industry (Hu and Quan 2006). Second, this metric tells management nothing about how well its money is being spent (Koch 2006). Third, it does not address IT's ability to use IT strategically (Kobelsky et al. 2006).

A second and increasingly strong external driver of IT spending is the regulatory environment within which a firm operates. Legislation, standards, and professional practices all affect what IT can and cannot do and how its work is done (Smith and McKeen 2006). These in turn affect how much is spent on IT and where it is spent (Hu and Quan 2006). Other external factors that have been shown to affect how much money is spent on IT include the following:

- ***Number of competitors.*** More concentration in an industry reduces the amount spent.
- ***Uncertainty.*** More uncertainty in a business's external environment leads to larger IT budgets.
- Diversification of products and services. Firms competing in more markets will tend to spend more on IT (Kobelsky et al. 2006). Internal factors affecting the size of the IT budget include the following:
- ***Affordability.*** A firm's overall performance and cash flow will influence how much discretion it has to spend on IT.
- ***Growth.*** Growing firms tend to invest relatively more in IT than mature firms.
- ***Previous year's spending.*** Firm spending on IT is unlikely to deviate significantly year to year (Hu and Quan 2006; Kobelsky et al. 2006).

## IT Processes

These are multilevel and complex and frequently occur in parallel with each other.

1. ***Set the functional IT budget.*** This budget documents spending as it relates to how IT organizations work—that is, what is to be spent on IT operations and how much is available to be spent on strategic investments. As noted above, the operations budget is relatively fixed and contains the lion's share of the dollars. In spite of this, IT managers must go through a number of machinations annually to justify this expenditure. Most IT organizations are still seen as cost centers, so obtaining budget approvals is often a delicate, ongoing exercise of relationship building and education to prevent inappropriate cost cutting (Koch 2006). Once the overall IT operations budget has been established, the challenge of allocating it to the individual business units remains, which, given the complexity of today's shared technical environment, is often a fixed or negotiated percentage of the total. Business units can resent these allocations over which they have no control, and at best they are viewed as a "necessary evil." In organizations where the IT operations budget is centralized, IT managers have greater opportunity to reduce expenses year by year by introducing standards, streamlining hardware and software, and sharing services. But in many companies, operations budgets are decentralized into the business units and aggregated up into the overall IT budget. This approach makes it considerably more difficult for IT managers to implement effective cost-reduction measures. Even in those firms that are highly effective and efficient, the relentless pressure from executives to do more with less makes this part of the annual budgeting process a highly stressful activity.

   Allocating the funds remaining to strategic investments is a completely separate process in which potential new IT projects are prioritized and their costs justified. Companies have many different ways of doing this, and most appear to be in a transition phase between methods of prioritization. Traditionally, IT organizations have been designed to parallel the organization structure, and new development funds have been allocated to business units on the basis of some rule of thumb. For example, each business unit might be allotted a certain number of IT staff and dollars to spend on new development (based on percentage of overall revenue) that would remain relatively stable over time. More recently, however, with greater integration of technology, systems, and data, there has been recognition of the cross-business costs of new development and of the need for more enterprise spending to address these. Increasingly organizations are moving to prioritize some or all new development at the enterprise level, thereby removing fixed allocations of new development resources from the business units.

   However it is determined, the strategic portion of the functional IT budget also involves staffing the initiatives. This introduces yet another level of complexity in that, even if the dollars are available, appropriate IT resources must also be available to be assigned to particular projects. Thus undertaking a new project not only involves cost justification and prioritization but also requires the availability of the right mix of skills and types of staff. Although some firms use fixed percentages of full-time, contract, and offshore staff in their projects, most use a more variable mix of employees and contract staff in their development projects in order to keep overhead costs low. As a result, creating new IT development budgets often involves a complementary exercise in staff planning.

2. ***Set the fiscal IT budget.*** A second, parallel stream of IT budgeting involves establishing the *fiscal* IT budget, which the CFO uses to implement the company's fiscal strategy and provide financial reports to shareholders and regulatory and tax authorities. This is seen largely by IT managers as a "translation" exercise where the functional IT budget is reconstituted into the operating and capital spending buckets. Nevertheless, it represents an additional "hoop" through which IT managers must jump before their budgets can be approved. In some companies capital funding is difficult to obtain and must be justified against an additional set of financial criteria. Some organizations require that IT capital expenditures be prioritized against all other corporate capital expenses (e.g., buildings, trucks), which can be a very challenging exercise. In other firms

CFOs are more concerned about increasing operating expenses. In either case this is an area where many IT managers set themselves up for failure by failing to "speak the language of finance" (Girard 2004). Because most IT managers think of their work in terms of operations and strategic investments, they are not mindful of some of the larger drivers of fiscal strategy such as investor value and earnings per share. To get more "traction" for their budgets, it is important for IT leaders to better translate what IT can do for the company into monetary terms (Girard 2004). To this end, many companies have begun working more closely with their internal finance staff and are seeing greater acceptance of their budgets as a result.

### Assess Actual IT Spending

At the other end of the budgeting process is the need to assess actual IT spending and performance. A new focus on financial accountability has meant that results are more rigorously tracked than in the past. In many companies finance staff now monitor business cases for all new IT projects, thus relieving IT of having to prove the business returns on what is delivered. Often the challenge of finding the right resources for a project or unexpected delays means that the entire available development budget is not spent within a given fiscal year. "We typically tend to spend about 85 percent of our available development budget because of delays or resourcing problems," said one manager. Hitting budget targets exactly in the strategic investment budget is a challenge, and current IT budgeting practices typically do not allow for much flexibility. On the one hand, such practices can create a "use it or lose it" mentality; if money is not spent in the fiscal year, it will disappear. "This leads to some creative accruals and aggressive forecasting," said the focus group. On the other hand, IT managers who want to ensure there is enough money for key expenditures create "placeholders" (i.e., approximations of what they think a project will cost) and "coffee cans" (i.e., unofficial slush funds) in their budgets. The artificial timing of the budget process combined with the difficulties of planning and estimation and reporting complexity, can lead to a distortion in the accurate reporting of what is spent.

## IT Budgeting Practices That Deliver Value

Although there is general agreement that current budgeting practices are flawed, there are still no widely accepted alternatives. Within IT itself, companies seem to be experimenting with ways to tweak budgeting to make it both easier and more effective. The following five practices have proven to be useful in this regard:

1. ***Appoint an IT finance specialist.*** Many companies now have a finance expert working in IT or on staff with the CFO working *with* IT. "Getting help with finance has really made the job of budgeting easier," said one manager. "Having a good partnership with finance helps us to leverage their expertise," said another. Financial specialists can help IT managers understand their costs and drivers in new ways. Within operations, they can assist with cost and value analysis of services and infrastructure (Gruman 2006) and also manage the "translation" process between the functional IT budget and the fiscal IT budget. "Finance helps us to understand depreciation and gives us a deeper understanding of our cost components," a focus group member noted. Finance specialists are also being used to build and monitor business cases for new projects, often acting as brokers between IT and the business units. "They've really helped us to better articulate business value. Now they're in charge of ensuring that the business gets the benefits they say they will, not IT." The improving relationship between finance and IT is making it easier to gain acceptance of IT budgets. "Having dedicated IT finance people is great since this is not what IT managers want to do," said a participant.

2 ***Use budgeting tools and methodologies.*** About half of the members of the focus group felt they had effective budgeting tools for such things as asset tracking, rolling up and breaking down budgets into different levels of granularity, and reporting. "We have a good, integrated suite of tools," said a manager, "and they really help." Because budgets serve so many different stakeholders, tools and methodologies can help "slice and dice" the numbers many ways, dynamically enabling changes in one area to be reflected in all other areas. Those who did not have good or well-integrated tools found that there were gaps in their budgeting processes that were hard to fill. "Our poor tools lead to disconnects all over the place," claimed an IT manager. Good links to the IT planning process are also needed. Ideally, tools should tie budgets directly to corporate strategic planning, resource strategies, and performance metrics, enabling a further translation among the company's accounting categories and hierarchy and its strategic themes and targets (Norton 2006).

3 ***Separate operations from innovation.*** Most IT managers mentally separate operations from innovation, but in practical terms maintenance and support are often mixed up with new project development. This happens especially when IT organizations are aligned with and funded by the business units. Once IT funds and resources are allotted to a particular business unit rather than to a strategic deliverable, it is very difficult to reduce these allocations. Agreement appears to be growing that operations (including maintenance) must be fully financially separated from new development in order to ensure that the costs of the first are fully scrutinized and kept under control while focus is kept on increasing the proportion of resources devoted to new project development (Dragoon 2005; Girard 2004; Gruman 2006; Norton 2006). Repeatedly, focus group managers told stories of how their current budget processes discourage accuracy. "There are many disincentives built into our budgeting processes to keep operational costs down," said one manager. Separating operations from innovation in budgets provides a level of visibility in IT spending that has traditionally been absent and that helps business unit leaders better understand the true costs of delivering both new development and ongoing services.

4. ***Adopt enterprise funding models.*** It is still rare to find organizations that provide corporate funding for enterprise wide strategic IT initiatives, yet there is broad recognition that this is needed (Norton 2006). The conflict between the need for truly integrated initiatives and traditional siloed budgets frequently stymies innovation, frustrates behavior designed for the common good, and discourages accountability for results (Hope and Fraser 2003; Norton 2006; Steele and Albright 2004). It is therefore recommended that more organizations will adopt enterprise funding models for at least some IT initiatives. Similarly, decentralized budgeting for core IT services is declining due to the cost-saving opportunities available from sharing these. Since costs will likely continue to be charged back to the differing business units, the current best practice is for IT operation budgets to be developed at an enterprise level.

5. ***Adopt rolling*** *budget cycles.* IT plans and budgets need attention more frequently than once a year. Although not used by many companies, an eighteen-month rolling plan that is reviewed and updated quarterly appears to be a more effective way of budgeting, especially for new project development (Hope and Fraser 2003; Smith et al. 2007). "It is very difficult to plan new projects a year in advance," said one manager. "Often we are asked for our 'best estimates' in our budgets. The problem is that, once they're in the budget, they are then viewed as reality." The artificial timing of budgets and the difficulty of estimating the costs of new projects are key sources of frustration for IT managers. Rolling budget cycles, when combined with integrated budgeting tools, should better address this problem while still providing the financial snapshots needed by the enterprise on an annual basis.

## Conclusion

Although IT budget processes have been largely ignored by researchers, they are a critical linchpin between many different organizational stakeholders: finance and IT, business units and IT, corporate strategy and IT, and different internal IT groups. IT budgeting is much more complex and difficult to navigate than it appears. In this chapter we have outlined some of the challenges faced by IT managers trying to juggle the realities of dealing with both IT operations and strategic investments while meeting the differing needs of their budget stakeholders. Surprisingly, very few guidelines are available for IT managers in this area. Each organization appears to have quite different corporate financial policies, which, in turn, drive different IT budgeting practices. Nevertheless, IT managers do face many common challenges in budgeting. Although other IT practices have benefited from focused management attention in recent years (e.g., prioritization, operations rationalization), budgeting has not as yet been targeted in this way. However, as business and IT leaders begin to recognize the key role that budgets play in implementing strategy and controlling costs, they will hopefully make a serious effort to address the budgeting issues faced by IT.

# CHAPTER 8

# Managing IT-Based Risk

Not so long ago, IT-based risk was a fairly low-key activity focused on whether IT could deliver projects successfully and keep its applications up and running (McKeen and Smith 2003). But with the opening up of the organization's boundaries to external partners and service providers, external electronic communications, and online services, managing IT-based risk has morphed into a "bet the company" proposition. Not only is the scope of the job bigger, but also the stakes are much higher. As companies have become more dependent on IT for everything they do, the costs of service disruption have escalated exponentially. Now when a system goes down, the company effectively stops working and customers cannot be served. Criminals routinely seek ways to wreak havoc with company data, applications, and Web sites. New regulations to protect privacy and increase accountability have also made executives much more sensitive to the consequences of inadequate IT security practices—either internally or from service providers. In addition, the risk of losing or compromising company information has risen steeply. No longer are a company's files locked down and accessible only by company staff. Today, company information can be exposed to the public in literally hundreds of ways. Our increasing mobility, the portability of storage devices, and the growing sophistication of cyber-threats are just a few of the more noteworthy means.

The job of managing IT-based risk has become much broader and more complex, and it is now widely recognized as an integral part of any technology-based work—no matter how minor. As a result, many IT organizations have been given the responsibility of not only managing risk in their own activities (project development, operations, and delivering business strategy, etc.), but also of managing IT-based risk in all company activities (e.g., mobile computing, file sharing, and online access to information and software). Whereas in the past companies have sought to achieve security through physical or technological means such as locked rooms and virus scanners, understanding is now growing that managing IT-based risk must be a strategic and holistic activity that is not just the responsibility of a small group of IT specialists but, rather, part of a mind-set that extends from partners and suppliers to employees and customers.

This chapter explores how organizations are addressing and coping with increasing IT-based risk. First we look at the challenges facing IT managers in the arena of risk management and propose a holistic view of risk. Next we examine some of the characteristics and components needed to develop an effective risk management framework and discuss a generic framework for integrating the growing number of elements involved in it. Lastly, we describe some successful practices organizations could use for improving their risk management capabilities.

## A Holistic View of IT-Based Risk

With the explosion in the past decade of new IT-based risks, it is increasingly recognized that risk means more than simply "the possibility of a loss or exposure to loss" (Mogul 2004) or even a hazard, uncertainty, or opportunity (McKeen and Smith 2003). Today, *risk* is a multilayered concept that implies much more is at stake.

> IT risk has changed. IT risk incidents harm constituencies within and outside companies. They damage corporate reputations and expose weaknesses in companies' management teams. Most importantly, IT risk dampens an organization's ability to compete. (Hunter and Westerman 2007)

As a result, companies are now focused on "enterprise risk management" as a more comprehensive and integrated approach to dealing with risk (Slywotzky and Drzik 2005). Although not every risk affecting an enterprise will be an IT-based risk, the fact remains that a large number of the risks affecting the enterprise have an IT-based component. For example, one firm's IT risk management policy notes that the goal of risk management is to ensure that technology failures or data integrity do not compromise the company's strategic objectives, the company's reputation and stakeholders, or its success and reputation.

In spite of the increasing number and complexity of IT-based threats facing organizations, it remains difficult to get senior executives to devote their attention (and commit the necessary resources) to effectively manage these risks. A global survey noted, "while the security community recognizes that information security is part of effective business management, managing information security risk is still overwhelmingly seen as an IT responsibility worldwide" (Berinato 2007). Another study of several organizations found that none had a good view of all key risks and 75 percent had major gaps in their approach to IT-based risk management (Coles and Moulton 2003). In short, while IT has become increasingly central to business success, many enterprises have not yet adjusted their processes to incorporate IT-based risk management (Hunter and Westerman 2007).

Knowing what's at stake, risk management is perennially in the top ten priorities for CIOs (Hunter et al. 2005), and efforts are being made to put effective capabilities and processes in place in IT organizations. However, only five percent of firms are at a high level of maturity in this area, and most (80 percent) are still in the initial stages of this work (Proctor 2007). Addressing risk in a more professional, accountable, and transparent fashion is an evolution from traditional IT security work. At a Gartner symposium the following was pointed out:

> Traditionally, IT security has been reactive, ad hoc, and technically-focused.... The shift to risk management requires an acceptance that you can't protect yourself from everything, so you need to measure risk and make good decisions about how far you go in protecting the organization. (Proctor 2007)

Companies in the group largely reflected this transitional state. "Information security is a primary focus of our risk management strategy," said one manager. "It's very, very visible but our business has yet to commit to addressing risk issues." Another stated, "We have a risk management group focused on IT risk, but lots of other groups focus on it too.... As a result, there are many different and overlapping views, and we are missing integration of these views." "We are constantly trying to identify gaps in our risk management practices and to close them," said a third.

There is, however, no hesitation about identifying the sources of risk. Every company in the group had its own checklist of risk items, and the experts have developed several different frameworks and categorizations that aim to be comprehensive (see Appendix A for some of these). What everyone agrees on is that any approach to dealing with IT-based risk must be holistic—even though it is an "onerous" job to package it as a whole. "Every category of risk has a different vocabulary," explained one focus group manager. "Financial, pandemic, software, information security, disaster recovery planning, governance and legal—each view makes sense, but pulling them together is very hard." Risk is often managed in silos in organizations, resulting in uncoordinated approaches to its management and to decision-making incorporating risk. This is why many organizations, including several in the focus group, are attempting to integrate the wide variety of issues involved into one holistic enterprise risk management strategy that uses a common language to communicate.

The connection among all of the different risk perspectives is the enterprise. Any IT problem that occurs—whether with an application, a network, a new system, a vendor, or a hacker (to name just a few)—has the increasing potential to put the enterprise at risk. Thus, a holistic view of IT-based risk must put the enterprise front and center in any framework or policy. A risk to the enterprise includes anything (either internal or external) that affects its:

- Brand
- Reputation
- Competitiveness
- Financial value
- End state (i.e., its overall effectiveness, efficiency, and success)

Figure 8.1 offers an integrated, holistic view of risk from an enterprise perspective. A wide variety of both internal and external IT-based risks can affect the enterprise. Externally, risks can come from the following:

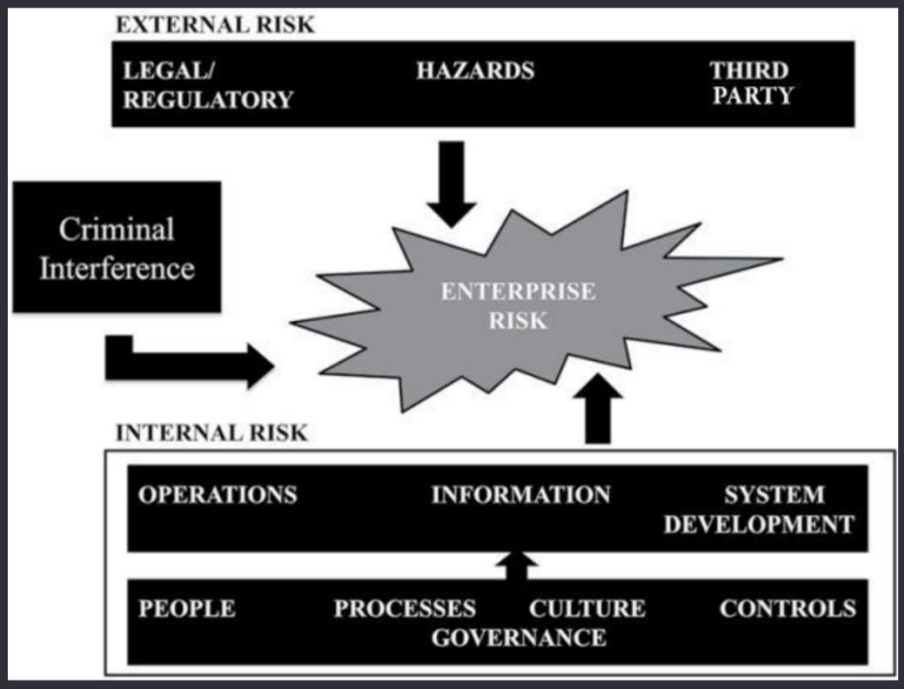


**Figure 8.1** A holistic view of IT-based risk

- Third parties, such as partners, software vendors, service providers, suppliers, or customers;
- Hazards, such as disasters, pandemics, geopolitical upheavals, or environmental considerations;
- Legal and regulatory issues, such as failure to adhere to the laws and regulations affecting the company, including privacy, financial reporting, environmental reporting, e-discovery, and so on.

Internally, some risks are well known, such as those traditionally associated with IT operations (availability, accessibility) and systems development (not meeting schedules or budgets or delivering value). Others are newer and, although they must be managed from within the organization, they may include both internal and external components. These include the following:

- Information risks, such as those affecting privacy, quality, accuracy, and protection;
- People risks, such as those caused by mistakes or lack of adherence to security protocols;
- Process risks, such as problems caused by poorly designed business processes or by failure to adapt business processes to IT-based changes;
- Cultural risks, such as risk aversion and lack of risk awareness;
- Controls, such as ineffective or inadequate controls to prevent or mitigate risk incidents;

- Governance, such as ineffective or inadequate structure, roles, or accountabilities to make appropriate risk-based decisions.

Finally, there is the risk of criminal interference, either from inside or outside the organization. Unlike other types of risk, which are typically inadvertent, criminal actions are deliberate attacks on the enterprise, its information, or sometimes its employees or customers. Such threats are certainly not new. Everyone is familiar with viruses and hackers. What is new, however, is that many more groups and individuals are targeting organizations and people. These include other national governments, organized crime, industrial spies, and terrorists. "These people are not trying to bring systems down, like in the past," explained a group member. "They are trying to get information."

## Holistic Risk Management: A Portrait

Tackling risk in a holistic fashion is challenging, and building an effective framework for its management will not occur overnight. It is therefore important to keep the big picture in mind, or the process could degenerate into overwhelming bureaucracy. It is interesting to note that there is much more agreement from the focus group and other researchers about what effective risk management *looks like* than how to do it. This section presents an impressionist portrait of what constitutes holistic risk management in order to show what this big picture should portray. A closer look at the detailed elements composing this picture will also be needed, but first it is essential that all people and functions involved in risk management agree on what image is being created. Otherwise, if one person is trying to create a Picasso while another is painting *Whistler's Mother*, it is unlikely that the resulting portrait will be pleasing to anyone!

With this in mind, we sketch some of the characteristics and components of a portrait of effective, holistic risk management:

1. ***Focus on what's important.*** "Risks are inevitable," admitted a manager. "The first question we must ask is, 'What are we trying to protect?'" said another. "There's no perfect package, and some residual risk must always be taken." A third added "Risks are inevitable, but it's how they're managed—our response, contingency plans, team readiness, and adaptability—that make the difference." In short, risk is uncertainty that matters, something that can hurt or delay an enterprise from reaching its objectives (Hillson 2008). Although many managers recognize that it's time to take a more strategic view of risk, "[W]e still don't have our hands around what's important and what we should be monitoring and protecting" (Berinato 2007). Risk management is not about anticipating all risks but about attempting to reduce significant risks to a manageable level (Austin and Darby 2003) and knowing how to assess and respond to it (Slywotzky and Drzik 2005). Yet, more than protecting the enterprise, risk management should also enable IT to take more risk in the safest possible way (Caldwell and Mogul 2006). Thus, the focus of effective risk management should not be about saying "no" to a risk, but how to say "yes," thereby building a more agile enterprise (Caldwell and Mogul 2006).
2. ***Expect the image to change over time.*** Few companies have a good grasp of risk management because IT is a discipline that is evolving rapidly (Proctor 2007). As a result, it would be a mistake to codify risk practices and standards too rapidly, according to the focus group. Efforts to do this have typically resulted in "paperwork without context," said one manager. Group members agreed that within a particular risk category, risk management actions should be "continuous, iterative, and structured." In recognition of this reality, most participant organizations have a mandatory risk assessment at key stages in the development process to capture the risk picture involved with a particular project at several points in time. Many also have regular,

ongoing reviews of required operational controls on an annual or biannual basis to do the same thing. In addition, when incidents occur, there should always be a process for evaluating what happened, assessing its impact, and determining if controls or other management processes need to be adapted (Coles and Moulton 2003). Finally, organizations should be continually attempting to simplify and streamline controls wherever possible to minimize their burden. This is a process that is often missed, admitted one manager.

However, despite the fact that each of these steps is useful in keeping one aspect of the risk picture in mind, it is also essential to stand back from these initiatives and see how the whole image is developing. It is this more strategic and holistic view that is often missing in organizations and that firms often fail to communicate to their staff. One of the greatest risks to organizations comes from employees themselves, not necessarily through their intentional actions, but because they don't recognize the risks involved in their actions (Berinato 2007). Therefore, many believe it is time to recognize that risk cannot be managed solely through controls, procedures, and technology but that all employees must understand the concepts and goals of risk management because the enterprise will always need to rely on their judgment to some extent (Symantec Corporation 2007). In the same vein, many managers also need to better understand this risk picture because they frequently do not comprehend the size and nature of the risks involved and thus resource their management inappropriately (Coles and Moulton 2003). As a result they tend also to delegate many aspects of risk management to lower levels in the organization, thus preventing the development of any longer-term, overall vision (Proctor 2008; Witty 2008).

3. ***View risk from multiple levels and perspectives.*** Instead of dealing with security "incidents" in a one-at-a-time manner, the group's managers are trying to do a better job of root cause analysis and understanding risks in a more multifaceted way. To date, risk management has tended to focus largely on the operational and tactical levels, but the managers suggest that risk management should also be viewed in a strategic way. One manager explained, "We need to assess risk trends and develop strategies for dealing with them. Tactics for dealing with future threats will then be more effective and easier to put in place." Another noted, "We must aim for redundancy of protection—that is, multiple layers, to ensure that if one layer fails, others will catch any problems."

   Furthermore, risk, security, and compliance are often intermixed in people's minds. Each of these is a valid and unique lens through which to view risk, with the challenge arising when all three are seen as being the same. For example, one expert noted that 70 percent of a typical "security" budget is spent on compliance matters, not on protecting and defending the organization (Society for Information Management 2008), and this imbalance means that overall spending in many firms is skewed. One firm uses the "prudent man" rule to deal with risk, which recommends a diversity of approaches—being proactive, prevention, due diligence, credibility, and promoting awareness—to ensure that it is adequately covered and that all stakeholders are properly protected. Monitoring and adapting to new international standards and laws, completing overall health checks, and analysis of potential risks are other new dimensions of risk that should be incorporated into a firm's overall approach to risk management.

## Developing a Risk Management Framework

With the big picture in mind, organizations can begin to develop a framework for filling in the details. The objective of a risk management framework (RMF) is to create a common understanding around risk, to ensure that the right risks are being addressed at the right levels, and to involve the right people in making risk decisions. An RMF also serves to guide the development of risk policies and integrate appropriate risk standards and

processes into existing practices. No company in the focus group had yet developed a comprehensive framework for addressing IT-based risk, although many had significant pieces in place or in development. In this section, we attempt to piece these together to sketch out what an RMF might contain.

An RMF should serve as a high-level overview of how risk is to be managed in an enterprise and can also act as a structure for reporting on risk at various levels of detail. Many companies have created risk management policies to guide staff about how IT risk and security are to be treated and all staff are required to read and sign them. Unfortunately, such policies are typically so long and complex as to be overwhelming and ineffective. "Our security policy alone is two hundred pages. How enforceable is it?" complained a manager. Another noted that the language in his company's policy was highly technical, which resulted in considerable noncompliance in following the recommended best practices. A plethora of committees, review boards, councils, and control centers are often designed to deal with one or more aspects of risk management, but they actually contribute to the general complexity of managing IT-based risk in an organization.

It should not be surprising that this situation exists, given the rapidity with which technologies, interfaces, external relationships, and dependencies have developed within the past decade. Organizations have struggled to simply keep up with the waves of legislation, regulation, globalization, standards, and transformation that seem to continually threaten to engulf them. An RMF is thus a starting point for providing an integrated, top-down view of risk, defining it, identifying those responsible for making key decisions about it, and mapping which policies and standards apply to each area. Fortunately, current technology makes it easy to offer multiple views and multiple levels of this information, enabling different groups or individuals to understand their responsibilities and specific policies in detail and see links to specific tools, practices, and templates, while facilitating different types of reporting to different stakeholders at different levels. By mapping existing groups, policies, and guidelines into an RMF, it is easier to see where gaps exist and where complexities in processes should be streamlined.

A basic RMF includes the following:

- *Risk category.* The general area of enterprise risk involved (e.g., criminal, operations, third party, etc.);
- *Policies and standards.* These state, at a high level, the general principles for guiding risk decisions, and they identify any formal corporate, industry, national, or international standards that should apply to each risk category. For example, one company's policy regarding people states the following, in part:

  > Protecting the integrity and security of client and corporate information is the responsibility of every employee. Timely and effective reporting of actual and suspected privacy incidents is a key component of meeting this responsibility. Management relies on the collective experience and judgment of its employees.

Another company policy regarding culture states, "We need to embed a risk management focus and awareness into all processes, functions, jobs, and individuals."

- *Risk type.* Each type of risk associated with each category (e.g., loss of information, failure to comply with specific laws, inability to work due to system outages) needs to be identified. Each type should have a generic name and definition, ideally linked to a business impact. Identifying all risk types will take time and probably require much iteration as "there are an incredible variety of specific risks" (Mogul 2004). However, developing lists and definitions is a good first step (Baccarini et al. 2004; Hillson 2008; McKeen and Smith 2003) and is already a common practice among the focus group companies, at least for certain categories of risk.

- *Risk ownership.* Each type of risk should have an owner, either in IT or in the business. As well, there will likely be several stakeholders who will be affected by risk-based decisions. For example, the principal business sponsor could be the owner of risk decisions associated with the development or purchase of a new IT system, but IT operations and architecture as well as the project manager will clearly be key stakeholders. In addition to specialized IT functions, such as IT security, audit and privacy functions in the business will likely be involved in many IT risk-based decisions. Owners and stakeholders should have clear responsibilities and accountabilities. In the focus group, some major risk types were owned by committees, such as an enterprise risk committee; or the internal audit, social responsibility, and risk governance committee; or the project risk review council on which stakeholder groups were represented.
- *Risk mitigation.* As an RMF is developed, each type of risk should be associated with controls, practices, and tools for addressing it effectively. These fall into one of two categories: compulsory and optional. Group members stressed that overemphasis on mitigation can lead to organizational paralysis or hyper-risk sensitivity. Instead, participants stressed the role of judgment in right sizing mitigation activities wherever possible. "Our technology development framework does not tell you what you have to do, but it does give you things to consider in each phase," said one manager. "We look first at the overall enterprise risk presented by a project," said another, "and develop controls based on our evaluation of the level and types of risk involved." The goal, everyone agreed, is to provide a means by which risks can be managed consistently, effectively, and appropriately.
- *Risk reporting and monitoring.* This was a rather controversial topic in the focus group. Although everyone agreed it is important to make risk and its management more visible in the organization, tracking and reporting on risk have a tendency to make management highly risk averse. One manager said:

  > We spent a year trying to quantify risks and developing a roll-up report, but we threw it away because audit didn't understand it and saw only one big risk. This led to endless discussion and no confidence that IT was handling risk well. Now we use a very simple reporting framework presenting risk as high, medium, or low. This is language we all understand.

  There are definitely pressures to improve risk measurement (Proctor 2007), but clearly care must be taken in how these metrics are reported. For example, one company uses a variety of self-assessments to ensure that risks have been properly identified and appropriate controls have been put in place. However, as risk management procedures become better understood and more codified, risk reporting can also become more formalized. This is occuring at present with operational process controls and fundamental IT security, such as virus or intrusion detection.

Risk monitoring is an ongoing process because levels and types of risk are changing continually. Thus an RMF should be a dynamic document that changes as new types of risk are identified, business impacts are better understood, and mitigation practices evolve. "We need to continually monitor all categories of risk and ask our executives if the levels of risk are still the same," said a focus group member. It is clear that failure to understand how risks are changing is a significant risk in itself (Proctor 2007). It is therefore especially important to have a process in place to analyze what happened when an unforeseen risk does occur. Unless efforts are made to understand the root causes of a problem, it is unlikely that effective mitigation practices can be put in place (Austin and Darby 2003).

## Improving Risk Management Capabilities

Risk management in most areas does not yet have well-documented best practices or standards in place. To that end, the focus group identified several actions that could lead to the development of effective risk management capabilities:

- ***Look beyond technical risk*** One of the biggest inhibitors of effective risk management is too tight a focus on technical risk, rather than on business risk (Coles and Moulton 2003). A traditional security approach tends to exclude this, often focusing only on technical threats or specific systems or platforms.
- ***Develop a common language of risk.*** A clearer understanding of business risk requires all stakeholders—IT, audit, privacy, legal, business managers—to speak the same language and use comparable metrics—at least at the highest levels of analysis where the different types of risk need to be integrated.
- ***Simplify the presentation.*** Having a common approach to discussing or describing risk is very effective, said several focus group members. While the work that is behind a simple presentation may be complex, presenting too much complexity can be counterproductive. The most effective approaches are simple: a narrative, a dashboard, a "stoplight" report, or another graphic style of report.
- ***Match the approach to the level of risk.*** Risk management should be appropriate for the level of risk involved. The most effective practices allow for the adaptation of controls while ensuring that the decisions made are visible and the rationale is communicated.
- ***Standardize the technology base.*** This is one of the most effective ways to reduce risk, according to the research, but it is also one of the most expensive (Hunter et al. 2005).
- ***Rehearse.*** Many firms now have an emergency response team in place to rapidly deal with key hazards. But it is less common that this team actually rehearses its disaster recovery, business continuity, or other types of risk mitigation plans. One manager noted that live rehearsals are essential to reveal gaps in plans and unexpected risk factors.
- ***Clarify roles and responsibilities.*** With so many groups in the organization now involved in managing risk in some way, it is critical that roles and responsibilities be documented and communicated. Ideally, this should be in the context of an RMF. However, even if an RMF is not in place, efforts should be made to document which groups in the organization are responsible for which types of enterprise risk.
- ***Automate 'Mere appropriate.*** As risk management practices become standardized and streamlined, automated controls begin to make sense. Some tools can be very effective, noted the focus group, provided they are applied in ways that facilitate risk management, rather than becoming an obstacle to productivity.
- ***Educate and communicate.*** Each organization has its own culture, and most need to work with staff, business managers, and executives to make them more aware of risk and the need to invest in appropriate management. Some organizations, like one insurance company in the focus group, are so risk-phobic that they need education to enable them to take on more risk. Such companies could benefit from better understanding their "risk portfolio" of projects (Day 2007). Such an approach can often help encourage companies to undertake more risky innovation initiatives with more confidence.

## Conclusion

Organizations are more sensitized to risk than ever before. The economy; the regulatory and legal environment; business complexity; the increasing openness of business relationships; and rapidly changing technology have all combined to drive managers to seek a more comprehensive understanding of risk and its management

(Rasmussen 2007). Whereas in the past risk was managed in isolated pockets by such functions as IT security, internal audit, and legal, today recognition is growing that these arenas intersect and affect each other. And IT risk is clearly involved in many types of business risk these days. Criminal activity, legal responsibilities, privacy, innovation, and operational productivity, to name just a few, all have IT risk implications. As a result, organizations need a new approach to risk, one that is more holistic in nature and that provides an integrative framework for understanding risk and making decisions associated with it. Accomplishing this is no simple task, so developing such a framework will likely be an ongoing activity, as experts in IT and others begin to grapple with how to approach such a complex and multidimensional activity. In this chapter we have not tried to present a definitive approach to risk management. There is general agreement that organizations are not ready for this. Instead, we have tried to sketch an impression of how to approach risk management and what an effective risk management program might look like. IT managers and others have been left to fill in the details and complete the portrait in their own organizations.

# CHAPTER 9

# Managing IT-Based Risk

There is no doubt that a strong business—IT relationship is now critical to the success of an organization's strategic and effective use of IT (Bassellier and Benbasat 2004; Kitzis and Gomolski 2006). With the rapid evolution of IT in business, simply "keeping the lights on" and delivering systems on time and on budget are not enough. Today, IT's ability to deliver value is closely linked with the nature of its relationship with a large number of business stakeholders. Recognizing this, many IT functions have tried to become "partners" with the business at the most senior strategic levels, although with limited success (Gordon and Gordon 2002). It has become clear from these initiatives that business—IT interactions are more complex and more highly resistant to change than first assumed and that building a strong relationship with business is a major challenge for most IT leaders.

We know that the nature and quality of the business—IT relationship are affected by many factors such as the subfunction of IT involved (e.g., operations, application development), the business unit involved, the management levels involved, changing expectations, and general perceptions of IT (McKeen and Smith 2008). However, research suggests that IT managers are still somewhat naïve about how relationships work in business and that interpersonal interaction and clear communication are often missing between the groups. We have also learned that perceptions of the value IT delivers are correlated with how well IT is perceived to understand and identify with the business (Anonymous 2002; Gold 2006; Tallon et al. 2000).

Nevertheless, we still know very little about the elements that contribute to a strong relationship between IT and business, or even about how to characterize such a relationship (Day 2007). In this chapter we first look at the nature of the business—IT relationship and how an effective relationship could be characterized. Then we examine each of the four foundational elements of a strong, positive relationship, and make suggestions for how IT managers could strengthen them.

## The Nature of the Business—IT Relationship

"The IT-business relationship is a set of beliefs that one party holds about the other and how these beliefs are formed from the interactions of ... individuals as they engage in tasks associated with an IT service" (Day 2007). The business—IT relationship in organizations tends to span the full range of relationship possibilities. Some members of the focus group felt they had generally healthy and positive relationships, and others labeled them negative or ineffective. Overall, "there's still a general perception that IT is slow, expensive, and gets in the way," said one manager. Even the focus group member with the most positive business—IT relationship admitted it was "not easy," and one set of researchers has described it as typically "arduous" (Pawlowski and Robey 2004).

Although "you can't have a one-sided relationship," as one focus group manager remarked, agreement is almost universal that IT needs to change if it is to improve. Literally dozens of articles have been written about what IT *should* be doing to make it better. For example, IT should better understand the fundamentals of business and aim to satisfy the "right" customers (Kitzis and Gomolski 2006); act as a knowledge broker (Pawlowski and Robey 2004); get involved in the business and be skilled marketers (Schindler 2007); manage expectations (Ross 2006); convince the business that it understands its goals and concerns and communicate in business language

(Bassellier and Benbasat 2004); and demonstrate its competencies (Day 2007). In short, "IT has to keep proving itself' to the business to demonstrate its value (Kaarst-Brown 2005). Thus practitioners and researchers both stress that cultivating a strong business–IT relationship is "a continuous effort" (a focus group member); "ongoing" (Luftman and Brier 1999); a "core IT skill" (Feeny and Willcocks 1998); and "emergent" (Day 2007).

On the business side of the relationship, two features stand out. First, business managers are often disengaged from IT work, according to both the focus group and researchers (Ross and Weill 2002). For example, in some cases in the focus group, IT staff have taken on business roles in projects in order to get them done. Second, it is clear that what business wants from this relationship is continually changing. "The business–IT relationship is cyclical," explained one manager. "The business goes back and forth about whether it wants IT to be an order taker or an innovator. Every time the business changes what it wants, the relationship goes sour."

So what *do* we know about the business–IT relationship in organizations? First, we know it is a multifaceted interaction of people and processes. It is unfortunately true that the existence of positive relationships between individual business and IT professionals does not necessarily mean that interactions will be positive on a particular development project, with the IT help desk, with an individual business unit, or between IT and the business as a whole (McKeen and Smith 2008). Because relationships manifest themselves in so many ways—formal and informal, tacit and explicit, procedural and cultural—we must recognize that their complexity means that they don't lend themselves to simplistic solutions (Day 2007; Guillemette et al. 2008; Ross 2006).

Second, we know that difficult, complex relationships often exhibit lack of clarity around expectations and accountabilities and have difficulty with communication (Galford and Drapeau 2003; Pawlowski and Robey 2004). This in turn leads to lack of trust. In the business–IT relationship, "complexity often arises when expectations differ in various parts of an organization, leaving a CIO with the difficult task of reconciling them and elucidating exactly what the IT function's mission and strategic role should be" (Guillemette et al. 2008). Several focus group members complained that different parts of their business expect different things from IT. "In some parts of our business, they want IT to be an order-taker; in others, they want us to be thought leaders and innovators," stated one manager. Another noted, "We live in an age of unmet expectations. There's never enough resources to do everything the business wants us to do."

Third, assumptions by the business about IT tend to cluster into patterns. One researcher has identified five sets of assumptions: 1) IT is a necessary evil, 2) IT is a support, not a partner, 3) IT rules, 4) business can do IT better, and 5) business and IT are equal partners. Business leaders who espouse one of these sets will tend to have similar ideas about who should control IT's direction, how central IT is to business strategy, the value of IT skills and knowledge, how to justify IT investments, and who benefits from IT (Kaarst-Brown 2005). Building on this idea, another study has also shown that business–IT relationships tend to vary along similar patterns. Different organizations tend to adopt one of five IT value profiles and expect IT to behave in accordance with the profile selected (see Appendix A). Problems arise when the assumptions and value profiles espoused by IT conflict with those of the organization or a specific part of the organization. As a result, many disconnects are often present in the relationship. For example, although IT departments and organizations often seek to be a business partner, their participation in this way is not always welcomed by the business (Pawlowski and Robey 2004).

- Clearly defined expectations, governance models and accountabilities;
- Trust between the two groups;
- Articulation and incorporation of corporate and client values and priorities in all IT work;
- A blurred line between business and IT (i.e., no "us vs. them");

- IT dedicated to business success;
- IT serving as a trusted advisor to the business;
- Mutual recognition of IT value.

In short, a strong business—IT relationship is one where realistic, mutual expectations are clearly articulated and communicated through individual and procedural interactions and where both groups recognize that all facets of this relationship are important to the successful delivery of IT value.

**Characteristics of the Business—IT Relationship**

- IT has to keep proving itself.
- The business is often disengaged from IT work.
- Business expectations of IT change continually.
- The relationship is affected by the interaction of many people and processes at multiple levels.
- Clarity is often lacking around expectations and accountabilities.
- Business assumptions of IT tend to cluster.
- There are many disconnects between the two groups.

## The Foundation of a Strong Business—IT Relationship

Strong relationships do not simply happen. They are built over time, and if they are to deliver value for the organization, they must be built to endure (Day 2007). The focus group told several stories of how the business—IT relationship in their organization had deteriorated when a business or IT leader changed or when a project wasn't delivered on time. Because it can so easily become dysfunctional, constant attention and nurturing are needed at all levels, said the focus group. However, building a strong relationship is not easy to do. Although there is no shortage of prescriptions, the sustained nature of problems in this relationship suggests that some underlying root causes need to be addressed. Appendix B provides one organization's view of what is needed in this relationship.

We have suggested previously that four components must be in place in order to deliver real business value with IT: competence, credibility, interpersonal interaction, and trust. The focus group reviewed these components and agreed that they also form the foundation of a successful and effective business—IT relationship. The focus group saw that developing, sustaining, and growing a strong business—IT relationship in each of these areas is closely intertwined with IT's ability to deliver value with technology. Therefore, a consistent and structured initiative to strengthen the business—IT relationship in these dimensions will also lead to an improved ability to deliver value successfully (see Figure 9.1). In the remainder of this chapter, we look at these four components in turn, discussing in detail how each acts as an important building block of a strong business—IT relationship and suggesting how each could be strengthened.

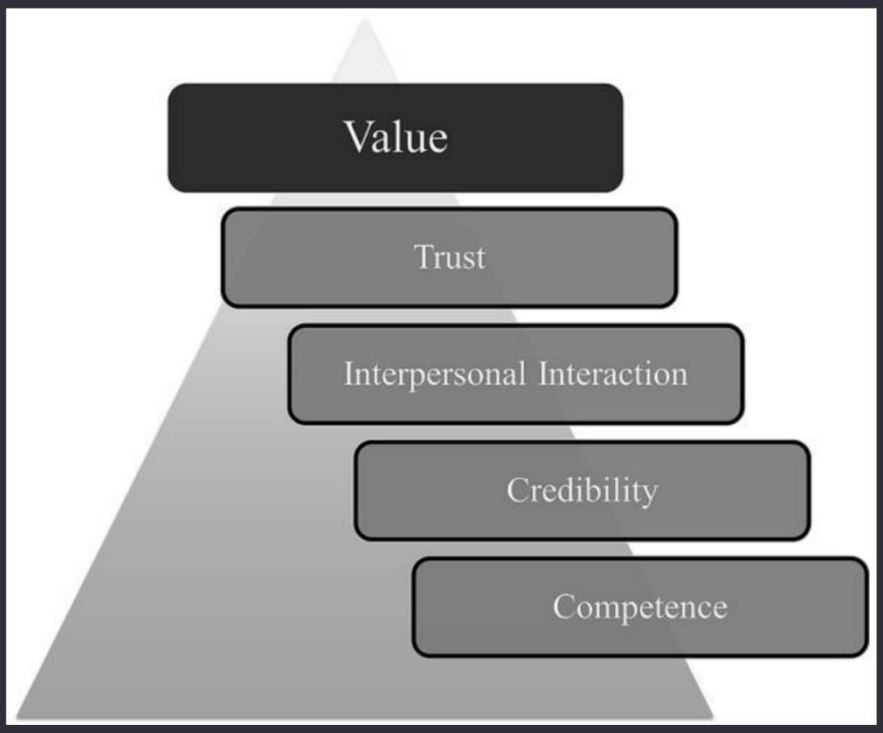


**Figure 9.1** Strong relationships are built on a strong foundation.

## Building Block #1: Competence

Although a competent IT organization that consistently delivers cost-efficient and reliable services is the bare minimum for an IT function, businesses today expect a great deal more of both their IT organizations and their IT professionals. Many IT organizations have adopted an internal service model in order to "operate IT like a business" and have demonstrated that they can provide services as effectively as external service providers, but these competencies fall short of what business now expects of IT (Kitzis and Gomolski 2006). Researchers and practitioners have identified a number of new competencies that are now required—to a greater or lesser extent—from all IT professionals.

First and foremost, IT staff need *business knowledge.* This goes beyond basic knowledge of a single business unit to include the "big picture" of the whole organization. IT personnel need to understand the business context in which their technologies are deployed, including organizational goals and objectives, capabilities, critical success factors, environment, and constraints. At all levels they need to be able to "think about and understand the development of the business as [any other business] member would and participate in making [it] successful in the same way" (Bassellier and Benbasat 2004). Furthermore, they need to be able to apply their business understanding to help the organization visualize the ways in which "IT can contribute to organizational performance and look for synergies between IT and business activities" (Bassellier and Benbasat 2004). In this regard, an important competence an IT department and its staff can bring to an organization is cross-domain and cross-functional business knowledge (Kitzis and Gomolski 2006; Wailgum 2008a).

Developing business knowledge does not mean that IT staff should become businesspeople but that they should be able to demonstrate they understand the business' goals, concerns, language, and processes and are working to help achieve them (Feeny and Willcocks 1998). One focus group organization surveyed its senior

managers about IT and found that these managers felt IT staff had a poor understanding of the business; as a result, they didn't trust IT's ideas.

Other key competencies which IT must cultivate include the following:

- ***Expertise.*** This includes having up-to-date knowledge, being able to support a technical recommendation, applying expertise to a particular business situation, and offering wise advice on risks, options, and trade-offs, as well as the ability to bring useful new ideas and external information (e.g., about new technologies or what the competition is doing with technology) to the business (Joni 2004; Pawlowski and Robey 2004).
- ***Financial awareness.*** Awareness of how IT delivers value and the ability to act in accordance with this value is a rare and prized skill (Mahoney and Gerrard 2007). All the focus group members felt pressure to continually demonstrate the business value of IT and recognized a strong need to make all IT staff more aware of such concepts as ROI, total cost of ownership, and how IT affects the bottom line and/or business strategy.
- ***Execution.*** It is not enough to understand the business and develop a vision; IT must also operationalize them. Since much of the business–IT relationship is dynamic—that is, continually being re-created every IT action speaks about its competence. It is well known that the inability to deliver an individual project on time and within budget will undermine the business's view of IT's overall competence. However, it is also the case that the actions of IT operations, the help desk, and other IT subfunctions will also be held up to similar scrutiny. As one focus group manager stated, "Poor delivery of *any* type can break a relationship."

In short, if the IT function is not seen to be competent at executing basic IT services or able to communicate in business terms, it will simply not be given an opportunity to participate in higher-order business activities, such as planning and strategy development (Gerrard 2006).

### Strengthening Competence

- ***Find ways to develop business knowledge in all IT staff.*** Focus group members use "lunch and learn" sessions, job shadowing, and short-term assignments in the business to accomplish this, but they recognize that more needs to be done to develop this competence.
- ***Link IT's success criteria to business metrics.*** This not only lifts IT's perspective to larger business concerns, but it also introduces all IT staff to the key financial and other measures that drive the rest of the organization.
- ***Make business value an explicit criteria in all IT decisions.*** Asking why the business should care about a particular IT decision, and how it will affect the business in both the long and short term, changes the focus of IT professionals in a subtle but very effective way, enabling them to communicate even technical decisions in business terms.
- ***Ensure effective execution in all IT activities.*** This ensures that IT sends a consistent message of competence to all parts and levels of the organization.

## Building Block #2: Credibility

Credibility is the belief that others can be counted on to do what they say they will do. It is built in many ways. Keeping agreements and acting with integrity, honesty, and openness are essential behaviors, whereas lack of timely and substantive responses and failure to observe deadlines can undermine it (Greenberg et al. 2007; Feeny et al. 1992). Focus group managers concurred that credibility is very important to the business—IT

relationship. Although in earlier days credibility was largely about the ability to deliver systems on time and on budget, now earning and maintaining credibility with the business has become more complex. Today's IT projects often involve many more elements (e.g., multiple platforms, risk management, adherence to laws and standards) and stakeholders than in the past, and the methods and tools of delivery are constantly changing. Furthermore, new research shows that it is typically the "little things" that can be most significant in undermining credibility and that people often make decisions based on IT's attention or inattention to such details (Buchanan 2005). One study concluded that "each and every IT service incident and event must be considered for its long-term influence" (Day 2007).

IT staff often assume that because they are *competent* they will be *credible*, but this is an invalid assumption. A recent survey of CIOs found that they wished their developers "didn't appear so clueless to the rest of the organization" (Wailgum 2008b). It is essential, therefore, that competence be *demonstrated* in order for others to feel someone is credible (Ross 2006). This is especially important in relationships where there is little face-to-face interaction. In these cases in particular, work must be visible and communication constant in order to demonstrate credibility (Hurley 2006).

### Strengthening Credibility

- ***Communicate frequently and explicitly.*** Make progress and accomplishments visible in clear and nontechnical ways. Focus group members found that when difficult decisions are planned together and clearly articulated in advance, much less tension develops in the relationship.
- ***Pay attention to the "little things."*** Wherever possible, take steps to provide prompt feedback and responses to queries and to ensure consistently high-quality service encounters.
- ***Utilize external cues to credibility.*** Examples include awards, endorsements from third parties, and the experience and background of IT staff. These specifics can be very useful when starting a new relationship with the business
- ***Assess all business touch points.*** All focus group members stressed the need to really listen to what the business says about its expectations and the problems it feels exist in the relationship. Just the effort alone sends a strong and positive message about the importance of this relationship, said a manager. However, he also stressed that undertaking such a review creates expectations that changes will be made, so regular reports back to the business about what is being done to improve things are especially important.

## Building Block #3: Interpersonal Interaction

The business–IT relationship is shaped by the development of mutual understanding, interests, and expectations, which are formed and shaped during a wide variety of interpersonal interactions (Gold 2006). Business–IT interactions must be developed and nurtured at many different levels in the business–IT relationship, said focus group managers, and although CEO–CIO interactions can set the tone for the relationship, the connections at multiple touch points contribute to its overall quality (Flint 2004; Prewitt 2005). The following are the four significant dimensions of interpersonal interaction:

- ***Professionalism.*** This is the unarticulated set of working behaviors, attitudes, and expectations that serves as the glue which keeps teams of diverse individuals working together toward the same goal. These behaviors are not only carefully watched by the business, they are also just as important *within* IT, said the focus group. Members noted that difficult internal IT relationships can lead to problems delivering effective IT services. Five sets of attitudes and behaviors contribute to developing IT professionalism: 1) comportment (i.e., appearance and manners on the job), 2) preparation (i.e., displaying competence and good organization), 3)

communication skill (i.e., clarity and etiquette), 4) judgment (i.e., the ability to make right choices for the organization), and 5) attitude (i.e., caring about doing a job well and about doing the right thing for the company) (McKeen and Smith 2008).

- ***Nontechnical communication.*** Over and over, research has found that the inability to communicate clearly with the business in its own terms can undermine the business–IT relationship (Bassellier and Benbasat 2004; Kitzis and Gomolski 2006). Today, because IT staff work across many organizational boundaries, they must also be effective at translating and interpreting needs—not only from business to technology and vice versa, but also between business units—in order to enable members of different communities to understand each other (Wailgum 2008a). Increasingly, as IT programs and services are delivered collaboratively by external partners and *to* external partners, clarity in communication is becoming mission critical.
- ***Social skills.*** The social dimension of the business–IT relationship is often ignored by both sides, leading to misunderstandings and lack of trust (Day 2007). Social bonds help diverse groups build trust and develop a common language, both of which are essential to a strong relationship. Socialization also helps build mutual understanding, enabling all parties to get comfortable with one another and uncovering hidden assumptions, which may become obstacles to success (Kaarst-Brown 2005). Socialization also develops empathy and facilitates problem solving (Feeny and Willcocks 1998).

Unfortunately, many IT organizations are structured in ways that create barriers between business and IT. For example, the use of "relationship managers" to act as interfaces between IT and the business is a mixed blessing. Although individually, these managers may be skilled and viewed positively by the business, focus group members noted that their position often leads them to act as gatekeepers to the business. One manager told of being hauled on the carpet to explain his lunch with a business manager (a personal friend), which hadn't been approved by the relationship manager! "We need a broad range of social interactions with the business," said another manager. "We use account managers, but we also encourage interactions through such things as lunches and social events." Ongoing, face-to-face interaction is the ideal, but with today's virtual teams and global organizations, other forms of social interaction, such as networking and collaboration tools, are being introduced to help bridge gaps in this area. In a virtual environment, social bonds can be more important than in a more traditional workplace, but they are harder to develop (Greenberg et al. 2007).

- ***Management of politics and conflict.*** The business–IT relationship can be turbulent, and IT personnel are not noted for their skills in dealing with the conflicts and challenges involved. Furthermore, conflict and politics tend to be exacerbated by the types of projects most commonly undertaken by IT—that is, those that cross internal and external organizational boundaries (Weiss and Hughes 2005). As a result, IT functions and personnel need ways to effectively address conflict and use it to deliver creative solutions. All too often, conflict is avoided or treated as a "hot potato" to be tossed up the management hierarchy (Weiss and Hughes 2005). Straight talk and the development of a healthy give-and-take attitude are fundamental to dealing with conflict at its source. Experts also recommend the development of transparent processes for managing disagreements and frank discussions of the trade-offs involved in dealing with problems (Pascale et al. 1997). These not only help stop damaging escalation and growing uncertainty but also help to model conflict-resolution skills for the staff involved.

Failure to understand the role of politics in a particular organization makes IT personnel less effective in their business interactions because they cannot craft "win–win" solutions. Thus, all IT staff need to understand something about politics and how it can affect their work. At more senior levels, it is imperative that IT

professionals learn how to act "wisely and shrewdly in a political environment" (Kitzis and Gomolski 2006). Since politics is part of every business relationship and cannot be avoided, IT personnel must learn how to work with it, said focus group members.

### Strengthening Interpersonal Interactions

- ***Expect professionalism.*** IT managers must not only articulate professional values and behaviors, they must *live* them and measure and reward them in their staff.
- ***Promote a wide variety of social interactions at all levels.*** Whether face-to-face or virtual, sharing information about each other's background and interests is an important way to bolster working relationships at all levels. Even where formal relationship managers are in place, IT leaders should encourage all IT staff to connect informally with their business colleagues. "Social interaction facilitates quick problem ownership and resolution and helps to develop a common language," said a focus group participant. Although the need for socialization increases as one moves up the organizational hierarchy, even at the lowest levels staff should be expected to spend about 10 percent of their time in this type of interaction (Kitzis and Gomolski 2006).
- ***Develop "soft skills" in IT staff.*** Although the need for interpersonal skills in IT has never been greater, many companies still give their development short shrift, preferring instead to stress technical competencies. In developing interpersonal skills, formal training should be only one component. It is even more important that IT managers take time to develop such skills in their staff through mentoring and coaching. Many focus group members have implemented "soft" skills development initiatives informally, but they also have admitted that the pressure to be instantly productive often detracts from both business and IT participation in them.

## Building Block #4: Trust

Effective interpersonal interactions, a belief that the job at hand will get done and get done right, and demonstrated business and technical competence are all required to facilitate trust that IT can be a successful partner with the business. But *even if* these are in place, proactive measures are still needed to actually *build* trust between the two groups. In many firms, an underlying sense of distrust of IT *as a whole* remains:

> IT's processes are notoriously convoluted and bureaucratic, leaving the business unsure of how to accomplish their business strategies with IT. From strategy alignment to prioritization to budgeting and resourcing to delivering value to managing costs, it must be clear that what IT is doing is for the benefit of the enterprise, not itself. (McKeen and Smith 2008)

The most important way to build trust at this level is through effective governance. The story of how one CIO managed to transform the business–IT relationship at Farm Credit Canada illustrates its importance:

> [At FCC, when Paul MacDonald became CIO], IT was considered a necessary evil. Business people were afraid of it and wished it would just go away.... [Transforming this relationship] was a very difficult and complex job—especially for cross-functional processes. Clear responsibilities and accountabilities had to be defined.... "It's all about clarity of roles and responsibilities," MacDonald said. The new IT governance model was validated and refined through sessions with key business stakeholders. "These sessions were important to demonstrate that we weren't just shuffling the boxes around in IT," [MacDonald] said.... MacDonald also made sure that the new model actually worked the way it was supposed to. "There were

cases where it didn't ... and with these, we made changes in our processes." He attributes his willingness to make changes where needed to his ability to make the new model actually function the way it was supposed to....

"Today, at FCC user satisfaction is very high and IT is seen as being indispensable...." [MacDonald] stressed that it is important to review and refine the new governance model continually. "There were some things that just didn't work," he said. "We are still constantly learning." (Smith and McKeen 2008)

Effective governance should be designed to build common business goals and establish a good decision-making process (Gerrard 2006). Mature processes in IT and transparency about costs develop trust (Levinson and Pastore 2005; Overby 2005). A focus group manager stated succinctly: "More transparency equals fewer surprises and you get transparency through governance." Aspects of governance that have enhanced trust in focus group organizations include integrated planning, defined accountabilities, a clear picture of mandates and authorities, and clarity around how work gets done.

Another focus group manager explained the importance of governance in this way:

In the past, we couldn't break the trust barrier. Now, [with an effective governance structure] we are more proactive and are fighting fewer fires. Our processes ensure proper escalation and a new focus on value. In short, governance captures the value of a good relationship and good fences make good neighbours.

Trust is essential for both superior performance and for developing the collaborative relationships that lead to success (Greenberg et al. 2007). It is developed through consistency, clear communication, willingness to tackle challenges, and owning up to and learning from mistakes (Upton and Staats 2008). Both inconsistent messages to stakeholders and inconsistent processes and standards can seriously undermine trust (Galford and Drapeau 2003).

Nevertheless, it must be stressed that there is no optimal form of governance (Gordon and Gordon 2002). The key is to develop a model of IT governance that addresses the business's *expectations* of its IT function. Thus, an IT organization can best build trust if it clearly understands the organization's priorities for IT and designs its governance model to match (Guillemette et al. 2008).

## Strengthening Trust

- ***Design governance for clarity and transparency.*** IT leaders should assess how the business views IT processes—from the help desk on up. It is important to recognize that all processes play a very visible role in how IT is viewed in the organization and that clear, effective, and fair processes are needed to break the "trust barrier" between business and IT at all levels.
- ***Mandate the relationship.*** Although it may seem counterintuitive, companies have had success from strictly enforcing relationship basics such as formal roles and responsibilities, joint scorecards, and the use of common metrics. Such structural measures can ensure that common expectations, language, and goals are developed and met.
- ***Design IT for business expectations.*** Clearly understanding the *primary* value the business wants IT to deliver can help IT understand how to focus its process and governance models (see Appendix A).

## Conclusion

There is clearly no panacea for a strong business–IT relationship. Yet the correlation between a good relationship and the ability to deliver value with IT makes it imperative that leaders do all they can to develop effective interpersonal and interfunctional business–IT relations. It is unfortunately still incumbent on IT leadership to take on the bulk of this task, if only because it will make IT organizations more effective. Business–IT relationships are complex, with interactions of many types, at many levels, and between both individuals and across functional and organizational entities. In this chapter we have not only identified and explored what a strong business–IT relationship should look like in its many dimensions, but we also have described the four major components needed to build it: competence, credibility, interpersonal skills, and trust. Unfortunately, business–IT relationships still leave a lot to be desired in most organizations. Recognizing that what it takes to build a strong business–IT partnership is so closely related to what is needed to deliver IT value may help to focus more attention on these mission-critical activities.