Two

The Three Core Disciplines of IT Risk Management

IMAGINE THAT you're the CEO (or CFO or CIO) of a large U.S. financial services company. For twenty years, the firm has grown rapidly through acquisitions and through the entrepreneurial actions of its seven autonomous business units. Now things are changing. Because growth is slowing, your team is shifting strategy from product-line growth to cross-selling, up-selling, and globalizing. Customers and business partners are starting to demand an integrated approach—asking your fiercely independent business units to look and act like a unified team. Worse, auditors are becoming a problem: your external auditors are paying more attention to IT, your regulators have begun IT-specific audits, and your business partners' auditors are now auditing you, too.

These strategic issues are linked closely to IT risks. You are sure some of the business units (but not all) have nagging availability and

access risks that they are not telling you about. Accuracy risk, which is under control within each business unit (or so you're told), is a significant problem now that customers and regulators are demanding accurate enterprisewide information. For example, it was difficult to certify financial reports for Sarbanes-Oxley, and accurate, up-to-date reporting of all activity with individual clients is more than a year away. Furthermore, you're having trouble convincing the top managers that they need to change the way they invest and work with IT. After all, each business unit president feels he gets enough agility from his dedicated IT staff and doesn't want to threaten his own unit's results to improve enterprise IT agility.

These are just the IT risks you can guess. There are surely more that you should know about but don't. You know you need to do something about IT risk—fast. But where do you start? Do you bring in a consulting firm to rewrite systems? Implement a strong management process to identify and fix every risk? Educate your business unit colleagues on the importance of IT risk and hope they'll change their own organizations?

Our research has defined a straightforward approach that answers these questions. In the simplest terms, IT risk management capability is built on three core disciplines. The three core disciplines work together as a cohesive whole to improve the enterprise's risk profile and keep it under control. They are:

- A well-structured *foundation* of IT assets—an installed technology base of infrastructure and application technologies, and supporting personnel and procedures, that is well understood, well managed, and no more complex than absolutely necessary
- A well-designed and executed *risk governance process* that provides an enterprise-level view of all risks, so that executives can prioritize and invest appropriately in risk manage-

ment, while enabling lower-level managers to independently manage most risks in their areas

- A *risk-aware culture* in which everyone has appropriate knowledge of risk and in which open, nonthreatening discussions of risk are the norm[1]

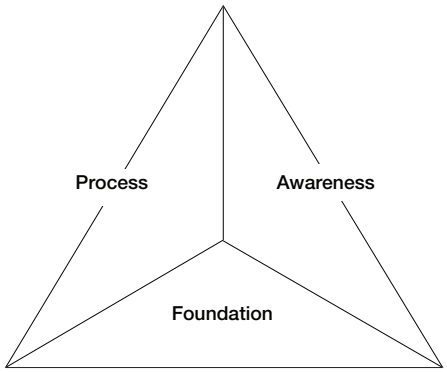
An enterprise that wants to make the most effective use of its scarce resources in managing IT risks must be competent in all three. But in any particular enterprise, some disciplines are an easier sell than others. Accordingly, many risk managers choose a focal discipline as a rallying point for risk management, using it to make the case for change and to improve all three disciplines over time. The choice of focal discipline depends on the enterprise's circumstances—including factors such as size, industry, and capabilities—and our research shows that successful IT risk management initiatives can begin with any of the three disciplines.

The three disciplines complement the 4A's. Discussing the 4A's sets a direction for the firm's IT risk management capability by specifying a desired risk profile and appropriate risk trade-offs. The three disciplines implement capabilities that shape the IT risk profile to match the enterprise's preferences on the 4A's. Then, closing the loop, the three disciplines provide information for further discussion and decision making at all levels of the enterprise.

Building the three disciplines does more than help the enterprise manage IT risks better. It also gives executives something that is all too often a luxury in a world of ever-increasing IT threats: confidence. You gain confidence that you know what your most important risks are, that you have an effective process to make decisions about those risks, and that managers throughout the organization have the ability to handle those risks effectively. In our study, firms that were more confident in their IT risk management capabilities reported more control over all four IT risks, were significantly less

FIGURE 2-1

The core disciplines of risk management



Source: © 2007 MIT Sloan Center for Information Systems Research and Gartner. Adapted from George Westerman, "Building IT Risk Management Effectiveness," Research Briefing IV(2C) (Cambridge, MA: Center for Information Systems Research, July 2004). Used with permission.

likely to say they were unaware of important IT risks, and enjoyed significantly better relationships between the IT organization and business executives—all while spending only a fraction more than other firms on IT risk management.

Figure 2-1 depicts the three disciplines as a triangle composed of three equal segments. The disciplines are complementary; each addresses different aspects of the 4A's by improving organization, technology, procedures, and behaviors. Together, they cover all the bases—improving risk management capability and giving business and IT people a language to ensure that IT risks stay under control.

Let's look at each of the three disciplines in more detail.

The Foundation

The foundation discipline addresses the 4A's in terms of technology and procedure by strengthening the *foundation*: that is, the collection

of IT assets, procedures, and people that support and enable business processes and decision making. This includes:

- Infrastructure that supports a wide range of computing, information management, and communications activities throughout the enterprise (this includes common technologies such as networks and computers, nonbusiness-process-specific applications such as e-mail and word processors, and common support functions such as an IT help desk)
- Applications that support the tasks and processes of the business, such as financial reporting systems, supply chain systems, and even the spreadsheets and decision support systems used by planners
- People with the skills to manage the foundation
- Processes and mechanisms for monitoring, control, and maintenance to keep these assets running smoothly and safely

As we said earlier, a solid IT foundation is well understood, well managed, and no more complex than absolutely necessary. A house built on a poor foundation suffers creaks, shakes, sagging, and eventual collapse. Owners must use heroic methods to prop up sagging floors and fix leaky plumbing caused by the structure's shifting over time. Organizations built on a shaky IT foundation are no different. Their owners are constantly propping up weaknesses and fixing leaks instead of enjoying the benefits of a well-built structure.

A solid IT foundation is risk resistant in many ways:

- *Problems are less likely.* Cracks and holes in the foundation are fixed through solid management processes. Intermittent and hidden bugs that are so common in complex systems are much less likely to be present.

- *When problems and failures happen, they are more quickly and easily diagnosed and repaired.* Lower complexity makes the causes of problems more apparent, and technical personnel are much more likely to understand what has gone wrong and how to fix the issue.

- *It is easier to assess risks.* The number of variables that bear on risk, such as the frailties and limitations of specific technologies or the detailed knowledge of specific configurations, is smaller. Monitoring and control processes are more easily configured to detect risky conditions.

- *It is easier to maintain.* Standardization allows technicians to make patches (i.e., fixes to things that weren't supposed to break to begin with) and upgrades using the same parts and procedures for all components, rather than having to understand different procedures for each component.

- *It is easier to change.* In a complex foundation, IT people must often change many components in many different places and then do extensive, complex testing to make sure all the changes work together. In a simplified foundation, change requires tinkering in fewer places, and testing can be done in a very straightforward way.

In short, a solid foundation avoids the opacity, complexity, frailty, and inattention that breed IT risk in most large organizations.

A Weak Foundation Amplifies All Risks

A weak foundation obviously creates risks related to availability and access. But the risks often go much further, impacting the company and its customers through threats to accuracy and agility. For example, one major insurance company's systems could not provide accurate, complete, and up-to-date information on policies and claims, which complicated customer service. An internal study showed that

the revenue loss from canceled policies was equivalent to the entire revenue from new premiums each year, and an incident involving poor customer service was the precipitating factor in over 80 percent of policy cancellations. The threat to long-term profitability was even greater, given that the typical insurance sales commission structure makes a policy unprofitable until it is several years old. Essentially, accuracy risks caused by a weak foundation and the resulting customer service problems forced the company to trade profitable current business for unprofitable new business—in effect, making it run faster and faster just to fall further and further behind. The study prompted executives to undertake a major transformation of the firm's IT foundation, not only as a risk control strategy, but as a growth strategy.

Fixing the Foundation Is a Journey

The first and most basic step to improving the foundation discipline is to examine the foundation and implement basic controls to ensure that there are no major weaknesses waiting to become catastrophes and to implement processes for recovery in the event of failure. The next step is to reduce complexity in infrastructure and applications, ultimately the most cost-effective way to reduce risk in the organization for the long term.

It is important to understand the terms *infrastructure* and *applications*: IT infrastructure is the platform that enables business applications to operate reliably; it consists of technical platforms (e.g., processing power, storage, networking, database, and middleware), people, nonbusiness-process-specific software such as e-mail or spreadsheets, and supporting services such as the help desk. Applications are the business-process-specific software that runs on the infrastructure.[2]

Although simplifying the foundation's infrastructure and applications requires up-front investment, which may be substantial, more substantial cost savings follow rapidly. In many cases significant initial steps toward simplification can be accomplished without dramatically

affecting business processes. This means that the impact of change on the enterprise can be minimized while risks *and* costs are reduced.

Almost any enterprise can succeed in simplifying its technology infrastructure, and the financial case alone is compelling, as we describe in our detailed discussion of the foundation discipline in chapters 3 and 4. But simplifying applications is much more costly, difficult, and disruptive to the entire organization. Therefore, making foundation simplification the centerpiece of IT risk management is usually feasible only when the business is able to build (or rebuild) its entire foundation of infrastructure and applications from scratch. This is, of course, what start-ups do, but relatively few established companies with inventories of existing legacy applications—aging, risky technologies whose continuing value to the business makes them difficult to abandon—are willing or able to do so. (The CIO of one government agency defined a *legacy system* for us as follows: "It's a system that's a hindrance in some way, but it's delivering business value, so you can't just get rid of it.")

When firms cannot start from a green field, they often choose a more gradual approach, changing the IT foundation chunk by chunk, beginning with infrastructure, and using each new business initiative to simplify a part of the applications. In this way, they gradually simplify, standardize, and strengthen the foundation.

In summary, the foundation discipline is the most cost-effective way to reduce IT risk. Immediately implementing controls and recovery processes reduces the likelihood and impact of risk in the current foundation. Simplification reduces both risk and ongoing maintenance and support costs. But in an enterprise with a substantial preexisting inventory of IT assets, the foundation discipline is the most difficult, time-consuming, and resource-intensive of the three disciplines. After the initial effort to bring the foundation to acceptable levels, firms with a large, complex inventory of applications typically choose to make either governance process or awareness, not foundation, their main focus. (For an overview of this discipline, see "A Summary of the Foundation Discipline.")

A Summary of the Foundation Discipline

The foundation is the collection of IT assets, procedures, and people that support and enable business processes and decision making. Bringing the foundation to a competent level—knowing what is in the foundation and ensuring that it is managed well—is essential for all enterprises. Many enterprises then work to make the foundation excellent by ensuring that it is only as complex as absolutely necessary.

Benefits of a foundation-driven approach:

- Immediately finding and fixing holes in the foundation corrects immediate weaknesses, providing time to make other longer-term improvements.
- Simplification is the most cost-effective risk management approach over the long term because it pays off in cost reduction as well as risk reduction.
- Simplification reduces all four IT risks and makes the other two disciplines easier to master.

Issues with a foundation-driven approach:

- Initial efforts to find and fix holes can be substantial.
- It can be difficult and costly to go beyond simplifying the infrastructure to simplify the applications.
- Simplification takes time. It is most often done incrementally.

We discuss the foundation discipline in detail in chapters 3 and 4.

The Risk Governance Process

The discipline of IT risk governance process addresses the 4A's organizationally and procedurally, ensuring that the organization has the necessary structures and processes to systematically identify and manage risks. This discipline creates and manages the processes, procedures, and organizational structures needed to:

- Define and maintain policy and standards
- Identify and prioritize risks
- Manage risks and monitor risk trends over time
- Ensure compliance with risk policy and standards

The risk governance process is the force that pulls otherwise fragmented, localized views of IT risk together into a comprehensive whole, allowing the enterprise to effectively set priorities and act. No centralized person or group has a wide enough perspective to fully understand and control all risks in even a moderate-sized organization. Local managers are best positioned to understand and manage risks in different parts of the organization. But even if those managers are aware of risk and engaged in managing it, their perspective is incomplete, and their priorities may differ from the enterprise as a whole. The organization needs mechanisms for local managers to identify and resolve risks *and* a consolidated view of risk that enables it to prioritize, invest in solutions, and monitor results at the enterprise level. The risk governance process is the means to both.

Most large enterprises lead their IT risk management with an effective risk governance process. For all enterprises, it is essential to be competent at this discipline as rapidly as possible.

When an enterprise's IT risk governance discipline is weak, the business has a fragmented, spotty view of risk. Some business units identify and handle risks much better than others. Audits are a re-

curring nightmare. Surprises are frequent. In the words of one CIO we interviewed, "I realized my biggest risk was that I didn't know what my IT risks were."

The fragmented view of risk that results from weak risk governance process carries significant dangers:

- *The full extent of a given risk and its priority compared to other risks are not understood.* Failure to address the most important risks first leads to dangerous exposures. Nearly all managers believe that their risks are the most important in the enterprise (or at least they say so)—but whose risks really matter most? Is a threat to availability in financial systems as important as the same risk in factory systems? How about the access, accuracy, and availability risks of computer virus attacks versus the agility risk of extending the integration period of a merger? Unless the enterprise has a process to examine and compare all IT risks, it can easily be distracted by the most visible and apparently urgent risk, whether or not that risk is the most important.

- *Spending and resources devoted to risk are not well understood.* Fragmentation hides the level of spending as well as the extent of risk. Our data shows that CIOs tend to seriously underestimate—by 100–200 percent on average—the amount of resources they devote to risk management. The most important reason for this miscalculation, we believe, is that the spending on risk management is compartmentalized—managed in multiple departments, by multiple managers, in multiple budgets.

- *The effectiveness of risk management efforts is not understood.* When risk oversight is fragmented, it's difficult to know whether efforts are producing the desired results and where, how, and why they are succeeding or failing. Many of the

people we surveyed for our study were concerned that they didn't know whether they were spending too much or too little on risk management; others were concerned that they weren't spending on the right things. Effective risk governance process eliminates much of that uncertainty.

- *Some risks are bigger than a single person or business unit.* When a person encounters an overwhelming risk and no help or support is available, his usual reaction is to push the risk to the back of his mind and try not to worry about it. (This, in a nutshell, is why life insurance, as the industry's conventional wisdom has it, is sold and not bought.) A risk governance process that manages risks up, down, and across the enterprise chain of command helps protect individual managers from risks whose impacts and solutions are beyond their personal scope of control—and from giving up and hoping that luck will solve the problem.

Finding the right type and balance of autonomy and control in a risk governance process takes experimentation in every enterprise. The right pace is important. In some enterprises risk governance benefits by starting loose and becoming tighter, while other enterprises may use tight risk governance to gain attention and rapidly reduce risks, easing the rigorous governance as awareness grows. All three risk management disciplines require resources, but the resources devoted to a risk governance process seem particularly onerous to many enterprises—especially those that demand provable ROI from every initiative. (As the global vice president of IT risk management in one major pharmaceutical company told us, "You can't prove that something never happened because of your IT risk management program.") Organizations that are historically immature in their processes or that are culturally hostile to visitors from headquarters who offer help may reject governance of any sort. Especially in smaller

businesses, the overhead associated with a risk governance process seems like a lot of trouble and expense. That said, a risk governance process tailored to enterprise needs is essential, since it is the only way to have a full view of the risks facing the enterprise.

For an overview of this discipline, see "A Summary of the Risk Governance Process Discipline." We discuss the risk governance process and considerations for its implementation in detail in chapter 5.

A Summary of the Risk Governance Process Discipline

Risk governance is the set of processes, policies, and structures that provide an enterprise-level view of all risks, so that executives can prioritize and invest appropriately in risk management, while it enables lower-level managers to independently manage most risks in their areas.

Benefits of a risk-governance-driven approach:

- It ensures an enterprisewide view of IT risk.
- It is best for integrating risk management with strategy.
- It highlights areas that are under- or overinvesting in risk.

Issues with a risk-governance-driven approach:

- There is potentially high overhead.
- If risk governance process is poorly managed, it can introduce bottlenecks and delays.
- It may be seen as just another administrative hurdle to jump (or avoid).

We discuss the risk governance discipline in detail in chapter 5.

A Risk-Aware Culture

The discipline of risk awareness addresses the 4A's in terms of personal responsibility and behavior. A risk-aware culture is one that has:

- Deep *expertise* in particular aspects of IT risk, which is typically held and used by specialists
- *Generalized awareness* throughout the enterprise of the nature and consequences of risky behavior and how to avoid them
- A *culture* that explicitly encourages everyone, at every level of the enterprise, to discuss risk openly and take personal responsibility for managing it

Regardless of how well structured its foundation is, no enterprise can manage risk well unless it has people who are aware of risk and willing to do something about it. Without deep expertise, basic technical and procedural protections can't be effectively implemented and managed. Without general awareness, people throughout the enterprise make easily preventable mistakes with serious consequences. Without a culture that encourages open discussion of risk and a shared responsibility for managing it, risky conditions are hidden from sight, or managers buffer themselves from risk with every means at their disposal.

Technology Only Goes So Far in Reducing Risk

At chemical company Hoechst/Celanese, whose case we discuss in detail in chapter 6, a risk-averse culture led project managers to ask for (and receive) far more money and time than they thought they would need as protection against unforeseen risks.[3] The managers always hit their targets. But their risk-averse culture increased risk to agility. The firm could not handle any but the most simple challenges quickly, a problem that became a survival issue when

major challenges appeared in the wake of a management buyout. The new management, in addition to improving the IT foundation, also undertook the challenge of changing the risk-averse culture to a risk-aware one.

Having good risk awareness is *not* about being risk averse. It's about being cognizant of risks and making smart decisions about them. Enterprises with a risk-aware culture take on more risks, but they're not more risky. They're just smarter about which risks they will take and how they will manage those risks.

Risk Awareness Is Built from the Top Down

A risk-aware culture demands that people sometimes prioritize enterprise risks above their own, that people share information about their risks and help others resolve their risks (often without personal gain), and that they sometimes take big, visible risks that have a chance of failure. This is not normal behavior in most large organizations, where incentives, policies, and politics generally favor risk aversion over smart risk awareness.

Only active engagement and support from the top of the enterprise can produce this kind of behavior. Executives in a risk-aware culture show—through their actions, investments, and behaviors—that risk management and the acceptance of calculated risk are part of the way the enterprise does business. This is not easy. It takes determination and focus to ask about the risks inherent in every new business initiative, to follow risk-related policies and governance rules even when it's difficult or inconvenient, to make risk an acceptable subject for conversation and occasional failure an acceptable (if not desirable) outcome.

Awareness is often the discipline of choice for smaller, agile enterprises, where the culture is already conducive to taking risks, sharing information, and helping each other. Even when large firms start with awareness (like EquipCo, whose story we tell in chapter 7),

they typically transition to a risk-governance-driven approach over time. For an overview of this discipline, see "A Summary of the Risk Awareness Discipline." We discuss the awareness discipline in more detail in chapter 6.

Every enterprise needs all three disciplines. A well-structured, well-managed IT foundation is inherently less risky than a more complex one. A risk-aware culture helps people recognize and deal openly with threats, risky behaviors, and risk reduction opportunities. And a mature risk governance process systematically develops a comprehensive picture of enterprise risks, bringing the full resources of the business to bear on risks that exceed the resources and authority of any single manager.

A Summary of the Risk Awareness Discipline

The risk awareness discipline builds an enterprise in which everyone, at every level, is aware of risk, discusses risk, and takes a personal responsibility for managing it. Risk-aware firms are characterized by a deep expertise in particular aspects of IT risk, which is typically held and used by specialists. They also build a generalized awareness throughout the enterprise of the nature and consequences of risky behavior, and encourage a culture in which risk is discussed and managed openly.

Benefits of an awareness-driven approach:

- Awareness is essential; even the best process can fail if it is built around uninformed people.

All three disciplines are necessary, but few enterprises give equal emphasis to all of them. Once dangerous conditions in the foundation are fixed, an enterprise can focus on the discipline that makes the most sense for the business. With that discipline as the driver, all three can be evolved into a stable, cohesive, comprehensive capability that systematically addresses the business trade-offs implicit in the 4A's.

Our research shows that most firms make either awareness or risk governance the focus of their programs, though there are good reasons to tackle the foundation first, as we describe in the next chapter. Whatever the focus, the goal is to embed risk management into the fabric of the enterprise. Effective risk management is achieved when risk management is part of the way that the enterprise does business—procedurally, technologically, organizationally, and behaviorally.

- Focused expertise helps the whole organization understand and resolve risks.
- Risk-aware culture improves willingness to discuss and manage risks as a team, rather than requiring individuals to fully manage their own risks.

Issues with an awareness-driven approach:

- It requires the visible attention of and role modeling from top executives; without their public support, effectiveness is limited.
- Awareness cannot be built by training alone; it must be incorporated into policy, processes, and culture.
- Companies can fail to achieve a balance between expertise and general awareness.

We discuss the risk awareness discipline in detail in chapter 6.