

A CIO's guide to IT risk management: tapping the extraordinary potential for business value and financial growth



Contents

2	<i>Introduction</i>
3	<i>The untapped opportunity in IT risk management</i>
4	<i>Taking a holistic view of risk</i>
5	<i>Remaking IT risk management</i>
10	<i>More CIOs can do to improve risk/return performance</i>
15	<i>Conclusion</i>

Introduction

Risk is an inherent part of doing business, and in a dynamic and global marketplace where change and uncertainty are the norm, risk rises exponentially. Corporate acquisitions, collaborative partnerships, global integration and accelerating technological advances all create risk, and today's most successful businesses have learned to absorb and mitigate it with relative ease. These companies are not only weathering change, they are taking advantage of it and, in some cases, even instigating it to uncover new opportunities. Such resilience is key to long-term growth and profitability.

With virtually every aspect of modern business linked to information technology (IT), resilience increasingly depends on a company's ability to effectively manage the risks introduced into its IT and physical infrastructure and processes. It's no wonder that for today's top CIOs, risk management is not just a dominant theme; it has become a vocation—just as it is for their business line colleagues. Still, the scope of many CIOs' risk management efforts is often too limited to gain real value for the business. The fact is, IT executives are more likely to practice risk avoidance than risk management. And when they focus too strictly on the risks to IT and overlook the risks and benefits to the business, they limit the opportunity to drive financial and operational advantage.

Good risk management in today's highly interconnected, dependency-driven business environment requires IT leaders to see and understand the business investment and financial upside of risk-taking. A holistic and more broad-based view of risk enables them to recognize the impact that IT processes and the infrastructure can have on business activities. They are better equipped to leverage IT's ability to reduce risks to the business and capitalize on opportunities for profit.

Highlights

The scope of many IT risk management efforts is often too limited to produce any real value for the business.

In an uncertain and constantly changing environment, taking risks and learning to mitigate them is essential to business growth.

A risk-aware governance framework facilitates this broader business perspective by providing decision makers across the organization with a more complete picture of risk and the potential for return. They gain the panoramic insight to make decisions that maximize revenue potential while levying an acceptable level of risk. They are better able to implement effective analysis and automation to address current risks while protecting the emerging interests of the enterprise. In short, they can achieve a better balance of risk and return.

CIOs who can communicate the business importance of risk management for IT and the related physical infrastructure can transform the way the IT leaders—and the entire enterprise—approach risk. More importantly, they can turn traditional IT risk management into a compelling, value-generating opportunity for the business.

The untapped opportunity in IT risk management

Companies that bring new products to market or invest in new ideas often do so at significant risk, but if they are successful—as many pharmaceutical companies and financial markets firms will attest—the payoff can be huge. Innovative companies understand that risk is essential to growing a business. Rather than try to eliminate it, these companies learn to thrive in an environment where outcomes are not certain, taking appropriate steps to mitigate the potential for loss.

CIOs as risk managers

IT and infrastructure risk management efforts rarely leverage risk for the purpose of creating advantage for the enterprise. There are several reasons, but most have to do with the narrow way in which IT leaders view and address risk. A siloed, asset-focused approach to IT risk management precludes them from looking end to end at business activities and revenue. Instead of viewing regulatory compliance as a means to prevent real threats to the business operation, they see it as a checklist of IT activities to be completed. They implement IT enhancements like virtualization and shared services to fix technical issues, without considering the business impact.

Who's on the line for risk management?

Despite IT's cultural aversion to risk-taking, CIOs are increasingly being assigned enterprisewide responsibility for risk management. In IBM's Global CFO Study 2008,¹ 25 percent of CFOs and other top financial leaders identified CIOs as the owners of risk, behind CFOs and CEOs. However, the study indicated that fewer CFOs and CEOs will have a risk ownership role in three years. Instead, CFOs expect more CIOs to be assigned that responsibility.

CIOs typically see operational stability, availability, protection and recovery plans as the end game for IT risk management. And while these are all good measures of IT risk management success, the part they play in the company's end-to-end business processes can be overlooked. IT leaders often fail to see the extent to which these objectives protect the business operation or how the safety net they provide empowers the business to expand into new markets, take on global partners and advance. They simply aren't used to looking at the IT operation with an eye toward reducing business risk or creating new revenue. After all, IT has historically been viewed as a cost center. As pressure to reduce IT costs continued to mount, CIOs were more inclined to use IT risk management to keep IT costs down rather than seek new ways to help the business reduce its operating cost and risk.

This perspective can make it difficult for CIOs to leverage IT for business gain. Valid growth opportunities can be missed, oftentimes because the associated risks are overestimated. The resulting inertia can be a real problem in a rapidly changing, global business environment. In IBM's Global CEO Study 2008, CEOs and other high-ranking business leaders expressed concern about standing still in such an environment.² Success capturing global opportunities depends on people's willingness to drive change, not just react to it. They must be willing to take risks.

Taking a holistic view of risk

With IT embedded in virtually every business activity today, there's no question that IT and related physical infrastructure risks underlie many of the risks facing the business. More and more, C-suite leaders are recognizing the need for improvements in IT risk management. The IT Governance Global Status Report—2008 from the IT Governance Institute found that 62 percent of the CEOs and CIOs surveyed implemented improvement measures in 2007 versus 45 percent in 2005 and 18 percent in 2003.³

However, a siloed approach to IT risk management can make any real improvement difficult. Traditionally, IT risks have been compartmentalized into tidy categories, like availability, access security and disaster recovery. The result is that interdependencies are not captured, and the total risk to a given

Highlights

A holistic approach to risk management enables IT leaders to get a complete picture of the potential threats and consequences to the business.

business activity or process can be miscalculated. This is not just important from a preservation perspective; it is also important from a growth perspective. Consider a technology upgrade aimed at increasing a bank's global business. With a siloed view of IT risk, it's not possible for business leaders to comprehend the actual risk posed by all of the potential threats to all of the bank's assets. Furthermore, there is no view that connects the bank's requirements for competitiveness and resilience to their respective dependencies in IT and the infrastructure. What's needed is a holistic, "all-hazards" view of risk for the enterprise.

A holistic view of risk enables IT leaders to connect the dots to the business. It provides a 360-degree vantage point, allowing them to see the vast array of potential threats to the business (natural, malicious, accidental and operational) and equally vast array of potential consequences to company assets and resources (people, information, hardware, software and facilities). They understand the continuum of risk, fully aware that seemingly small operational stability issues, like insufficient capacity, can turn into huge losses if unattended. Knowing the systems that each business activity depends on, IT leaders are better able to prioritize recovery times and identify how and when IT improvements should be implemented. Knowing the business benefits of desired IT risk mitigation initiatives, they are also better able to make a case to senior executives.

Remaking IT risk management

Clearly, CIOs should be moving towards a broader business-oriented approach to IT risk management. After all, it is a critical element in IT's strategic alignment with the business, enabling CIOs to operate in the risk/return world in which the rest of the C-suite lives.

A business-oriented approach looks at IT and related physical infrastructure risk management challenges from a business process perspective, identifying business risks by mapping business processes to IT-related sources of risk. Dependency analysis is used to identify the ways in which the business interacts with specific IT and infrastructure elements. By breaking down IT activities into layers, IT-related root causes can be more easily understood.

A holistic approach to IT risk management enables IT leaders to get a complete picture of the potential threats and consequences to the business.

Highlights

Dependency analysis enables companies to understand the IT-related root causes of potential business problems before those problems occur.

Benefits of process-based approaches to IT risk management

Process-based approaches enable organizations to become more aware of their gaps and the need for improvements in IT risk management. According to the IT Governance Global Status Report—2008, CEOs and CIOs using COBIT were more likely to rate IT risk management as “very important” than the general population (57 percent to 44 percent). With a greater emphasis on risk management, these companies are more likely to make the kinds of enhancements that drive business value.

One method involves evaluating the business process and outcome risks of IT activities. Potential business outcomes and associated risks are identified for each IT process. Using change management as a sample process, where changes can refer to technology changes (data center consolidations, new configurations) as well as business changes (acquisitions, cost-cutting), possible outcome risks could be downtime, lost data, system delays and insufficient capacity. These business outcomes are all indicative of IT process problems, including inadequate planning, accelerated deployment and lack of readiness. They can result from poor process design, poor execution (which could point to training problems), or an incorrect response when a problem does arise. The point is that negative business outcomes need to be traced back to their root causes, including process-related causes.

The importance of a structured governance framework

Good IT risk management is not possible without a strong governance framework. Governance provides the policies, controls and operational guidelines that enable IT leaders to manage risks and weigh their business value. But to provide benefit over the long term, a governance framework must be responsive to changing business conditions. Fortunately, several high-quality frameworks already exist, and CIOs can take immediate advantage of their standards and best practices for IT risk management.

Excellent guidance can be found in the globally accepted, open standards developed by the IT Governance Institute (ITGI™). Control Objectives for Information and related Technology (COBIT®) provides best practices for the governance of technology and the infrastructure, including risk management. While COBIT focuses on execution, ITGI's Val IT™ focuses on helping companies steer their IT-enabled business investments, including risk-related initiatives, for the greatest return.⁴ Other helpful guidance for IT risk management is available from the International Standards Organization (ISO) and the U.K. Office of Government Commerce's IT Infrastructure Library® (ITIL®), among others. IBM's Process Reference Model for IT (PRM-IT), Component Business Model for the Business of IT (CBM-BoIT) and Resilient Enterprise Blueprint tie these best practices together and provide a roadmap for implementation.

Highlights

CIOs should take a lead role in executing structured processes to improve IT's risk awareness and ability to prepare for, analyze and respond to risks.

In addition to boosting resilience, standards and best practices enable companies to better manage top-line financial risks. They can help companies avoid contractual, industry and regulatory penalties, and can improve their ability to win business and maintain existing contracts. Companies want to know that they can maintain operations in the face of a variety of threats; their customers want assurance that their information and other assets will be protected. Governance frameworks help meet these objectives.

While the standards and practices advocated by each framework may vary in terminology, their process recommendations for managing IT risk are generally the same:

- **Define the scope of risk analysis.** *Identifies the business activities, initiatives, and supporting technologies and infrastructure elements that will be included in the IT risk management effort.*
- **Identify and define risks.** *Maps each business activity to potential threats and the resources that could be at risk.*
- **Assess the likelihood of risk occurrence and level of impact.** *Calculates the probability and severity of an actual breach from the scope of business activities, resulting in an overall view of risk.*
- **Evaluate controls.** *Assesses the quality of existing controls used to prevent, detect and mitigate risks, factoring in cost versus value provided.*
- **Assess risk and determine treatments and responses.** *Reviews risks relative to risk appetite, then prioritizes risk reduction activities and selects investments based on cost/benefit analysis.*
- **Implement risk reduction actions.** *Develops, tests and implements detailed plans for risk treatment.*
- **Provide ongoing monitoring and feedback.** *Continually collects data on threats, impacts and effectiveness of current risk management processes, and adjusts risk action plans and processes accordingly.*

Highlights

Structured processes like these improve a company's proactive risk awareness and ability to prepare for, analyze and respond to threats. However, organizational complexity can make it difficult to implement them. With risk management an increasingly integral part of the CIO's job and a greater number of risks falling within IT's sphere of control, CIOs should take a lead role in executing these processes by:

- *Allocating adequate funding and resources for risk analysis initiatives*
- *Providing direction, fostering dialogue among stakeholders, and ensuring continuous alignment with business objectives and compliance with governance policies*
- *Striving for continuous process improvement*
- *Helping to incorporate greater risk awareness into the company's general business governance*
- *Establishing risk management policies to guide activity execution.*

The importance of people, organization and automation

Understandably, IT risk management programs that make potential business threats more visible and easier and less costly to respond to are likely to earn the most points with senior management. CIOs have a tremendous opportunity to produce these outcomes by overcoming the hurdles associated with people, the organization and automation:

Successful IT risk management programs depend on a risk-aware culture, executives who are heavily invested and automated processes to facilitate analysis and resolution.

- **People.** *To be truly effective, risk management must be more than a program—it must be deeply embedded into the corporate psyche of the workforce. Companies need to develop a risk-aware culture that is attuned to the wide range of potential threats facing the business as well as the risk-response strategy for mitigating them. Rather than focusing on recovery after the fact, risk training programs should focus on preparing employees to notice, identify and respond to risks. Every employee should feel empowered to preserve and create value for the business.*

Highlights

- **Organization.** *While executive support for IT risk management is a given, its effectiveness is not. Risk management processes, such as those provided by COBIT, must be combined with business continuity directives and risk-aware governance from the top down. Risk management must be strategically integrated into the fabric of the business in order to bridge the silos of risk and truly understand inter-organizational dependencies and the breakdowns that could compromise the business.*
- **Automation.** *Automation can facilitate IT risk management in two important ways. First, it can alleviate the complexity associated with vital risk analysis and reporting. The larger the organization and the more business and technological changes introduced into the organization, the more complicated these processes can be. Second, automation makes it easier to assess and reduce real risks to real operations. Business activity and service management applications, controls monitoring and security applications reduce the strain on resources, performing root-cause diagnostics and sense-and-respond functions. They can help identify threats, provide early warning, simplify and reduce the cost of responding to risks, and improve the consistency of risk management processes.*

The risk-related maturity of a company's people, executive organization and automation must be in alignment to derive the greatest business value from risk management initiatives.

Typically, improvements are needed in one or more of these areas; however, all three must be in continuous balance to enable effective IT risk management (Figure 1). Company-wide risk awareness, for example, can be improved through corporate education, but it doesn't necessarily provide employees with the processes to take productive action. Similarly, employees

Highlights

who have been trained in risk response processes will be unable to truly fix problems without sufficient automation. When the maturity levels of the three elements are out of alignment, companies are likely to derive little value from their investment in risk management. For the best results, companies need to make continuous improvements in all three.



Figure 1. Effective IT risk management depends on balanced investments in people, organization and automation.

Today, CIOs need to recognize that managing IT is about achieving the greatest return for the least amount of risk.

More CIOs can do to improve risk/return performance

With the CIO's increasingly strategic role in the C-suite, expectations for IT risk management are higher than ever. CIOs must understand the true cost of IT risks, and that means knowing full well the impact their decisions have on revenue, customer retention and competitive advantage. In a value-driven world, managing IT must be about achieving the greatest return for the least amount of risk (Figure 2).

Highlights

Risk budgeting enables CIOs to optimize business return by spending their risk capital in the most efficient way possible.

Adopt a risk budget

Risk budgeting provides a framework for determining which risks are worth taking. It enables CIOs to leverage the same principles financial leaders do, allocating sufficient risk resources to address “known” IT risks, such as availability, while leaving a greater risk budget for true business unknowns. Take, for example, decisions to build a new portal to lower customer churn or to provide excess capacity to cover anticipated transaction volumes for a newly released product. The steps taken to reduce the IT risks associated with these initiatives are much better understood than the actual customer acceptance rate of a new product or the effectiveness of a new distribution channel. Risk budgeting enables CIOs to work with business leaders to make resource allocation decisions that will improve return. By prudently spending resources to reduce IT risk, CIOs free business leaders to spend their risk budget on other, harder to manage, business risks associated with a new initiative.

Open the risk discussion

Managers don't like to talk about risk. It's easier and less disruptive to believe that every project will proceed according to plan and failures will never happen. In this risk-avoidant atmosphere, employees are justifiably reluctant to report problems that could significantly impact a project. Often, they wait too long, addressing risks after an IT solution is in production—and becoming unwitting heroes in the process. Companies with this kind of culture are forced to react to problems as they arise, often in crisis mode.

CIOs need to reach out to their colleagues for whom risk is top of mind and show how IT can proactively address risk and drive greater value for the business.

Most CIOs have enough project experience to know that “risk-free projects” simply don't exist. They are well aware that anticipating what can go wrong is better than waiting to react to it. By reaching out to colleagues for whom risk is top of mind—Chief Financial Officers, Chief Risk Officers, Business Continuity leaders—and beginning a dialogue, CIOs can increase risk awareness across the enterprise and foster a healthy risk culture that encourages prompt reporting of risks. Working with business lines and even external parties (investors, suppliers, customers, rating agencies, regulators), CIOs can explain how it's possible to work together to reduce IT risk and, more importantly, identify how IT can proactively address risk and drive greater value for the business.

Highlights

Risk-aware governance integrates risk teams from across the enterprise and makes risk and resilience everyone's job.

CIOs can help business leaders see the merits of a consolidated risk picture and bridge siloed risk discussions and programs.

Build a case for risk-aware governance

Continuous, proactive risk management is best accomplished through risk-aware governance. While governance can exist in many forms, risk-aware governance provides the most holistic view of risk, integrating risk teams from across the enterprise and making risk and resilience everyone's job. Employees understand the organizational dependencies that lead to risk and are better equipped to make everyday decisions that will positively impact the company's risk position. Business line leaders can see beyond their own organization's concerns, and they can prioritize investments and motivate the best course of action for the business. COBIT, Val IT and other governance frameworks guide and monitor these decisions, enabling employees to analyze risks in the context of their potential return.

Risk-aware governance makes it easier for business leaders to view IT risk management foundationally as a means to increase resilience or prevent threats to technology and the physical infrastructure, and then as a means to help the business achieve its growth objectives. Certainly CIOs have a vested interest in communicating this view of IT and related physical infrastructure risk management. The place to start is by eliminating the various silos of risk that exist within IT and delivering a unified perspective that identifies the interdependencies and the range of potential threats and impacts on business, technology and infrastructure assets.

Next, CIOs need to extend the risk unification logic to the rest of the business, making it easier for business line leaders to understand the array of risks facing their own business processes. Many simply aren't aware of the risks they face from other business areas or the risks they create for those areas. Seeing the whole picture is essential because it reveals key exposures, actual losses and trends. It also simplifies risk management because it eliminates separate silo-specific risk discussions.

For senior management, who must answer to shareholders and trustees, the importance of a consolidated risk picture cannot be overstated, and CIOs can help deliver this picture. As CFOs evaluate the merits of new projects and investments, CIOs can be helpful in illuminating the risks in CFOs' risk and return calculations. CIOs can also illustrate how less IT risk translates into greater operational stability, and ultimately greater financial stability.

Highlights

CIOs have the application knowledge and information to simplify risk analysis, monitoring and response.

Complex infrastructures and applications can introduce added risks without providing anticipated business benefits.

The right applications can simplify risk analysis and monitoring, and CIOs have the expertise to deploy them. Dependency analysis applications can help identify potential single points of failure and possible contention for shared resources. They can help business leaders understand the potential root causes of business risks, recognize patterns of risk and then take advantage of the early warning they provide. While the dependencies of a business activity, process or application are often not evident to business owners, CIOs' IT perspective enables them to see dependencies enterprisewide. CIOs can use predictive techniques to forecast risks, not just react to them. Plus, their knowledge of process improvement methodologies like Six Sigma can also go a long way toward reducing risk while establishing common ground with business lines that may already be using these applications.

Drive out complexity

Large IT and physical infrastructures are never simple, but many have become overly complex. Consider a typical infrastructure with multiple disparate platforms implemented to satisfy individual preferences rather than specific business requirements. They not only require more time and resources to maintain, they introduce risk without adding any clear business benefit. Complex applications can have the same effect, increasing the burden on management without delivering anticipated value.

CIOs often pay the price for IT complexity and the risks that result. Needless to say, no one should be more interested in simplifying the infrastructure. From consolidation and virtualization to service oriented architecture, CIOs interested in driving up return should take steps to drive out complexity.

Highlights

Building a platform for value creation through IT risk management

- ✓ Enable a single, holistic view of risk management by bridging the risk management silos across IT and the enterprise
- ✓ Increase the business' awareness of the range of potential threats and the range of potential impacts on assets and resources
- ✓ Leverage dependency analysis to expose the interconnections and root cause of risks
- ✓ Take advantage of the IT risk management guidance, open standards and best practices in structured governance frameworks
- ✓ Improve IT risk management through balanced improvements in people, organization and automation
- ✓ Establish a risk budget, allocating risk capital based on potential reward
- ✓ Connect with business leaders and external partners regularly to remove cultural barriers and keep the risk management discussion moving forward
- ✓ Communicate the importance of risk-aware governance
- ✓ Drive out the IT and infrastructure complexities that can increase risk and limit return

Figure 2. Steps to improving risk/return performance—a checklist for CIOs.

Proactive risk management not only enables business growth, it can enable CIOs' personal growth as well, expanding relationships, influence and credibility among the C-suite.

Leverage the leadership opportunity in IT risk management

CIOs have an opportunity to demonstrate business leadership by increasing IT's risk-return impact for CFOs and other business line leaders. In the right hands, IT risk management is a virtual hotbed for value creation, but CIOs have to change the way they approach risk or be willing to forego the growth opportunities that go along with it. Innovation and revenue growth aside, proactive risk management can result in personal growth as well, expanding CIOs' relationships, influence and strategic credibility with C-suite colleagues.

Conclusion

Most business leaders understand the connection between growth and risk. As CIOs reach for a greater role in the strategic circle, they need to look beyond IT and take a more comprehensive, business activity-based view of risk that is focused on opportunity creation, not just loss prevention. Eliminating IT's siloed approach to risk management is critical to extending IT's ability to deliver this kind of business value—and CIOs have a responsibility to lead this effort. With their application knowledge and enterprisewide visibility, they can help CFOs and business leaders see the potential for return embedded in IT risk management. What's more, by proactively promoting and implementing a risk-aware governance framework, CIOs can enable their companies to build business capabilities that mitigate crises while driving profitability and extraordinary business value.

For more information

For more information on IT risk management and value creation, contact Brian Barnier at bbarnier@us.ibm.com, call your IBM representative or IBM Business Partner, or visit:

ibm.com/cio



© Copyright IBM Corporation 2008

IBM Global Services
New Orchard Road
Armonk, NY 10589
U.S.A.

Produced in the United States of America
September 2008
All Rights Reserved

IBM, the IBM logo, and **ibm.com** are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

ITIL is a registered trademark, and registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Other company, product and service names may be trademarks or service marks of others.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

¹ IBM, *Balancing Risk and Performance with an Integrated Finance Organization: The Global CFO Study 2008*, October 2007. www.ibm.com/gbs/2008cfostudy The Global CFO Study 2008 was developed in cooperation with The Wharton School at the University of Pennsylvania and Economist Intelligence Unit.

² IBM, *The Enterprise of the Future: The Global CEO Study 2008*, June 2008. www.ibm.com/ibm/ideasfromibm/us/ceo/20080505/index.shtml

³ IT Governance Institute, *IT Governance Global Status Report—2008*, 2008. www.itgi.org/AMTemplate.cfm?Section=ITGI_Research_Publications&Template=/ContentManagement/ContentDisplay.cfm&ContentID=39735
The IT Governance Global Status Report—2008 is based on a global survey of CIOs and CEOs conducted by PricewaterhouseCoopers for the IT Governance Institute (www.itgi.org/).

⁴ SovIT® and Val IT™ are made freely available as open standards by the IT Governance Institute.



Recyclable, please recycle

CIW03045-USEN-00