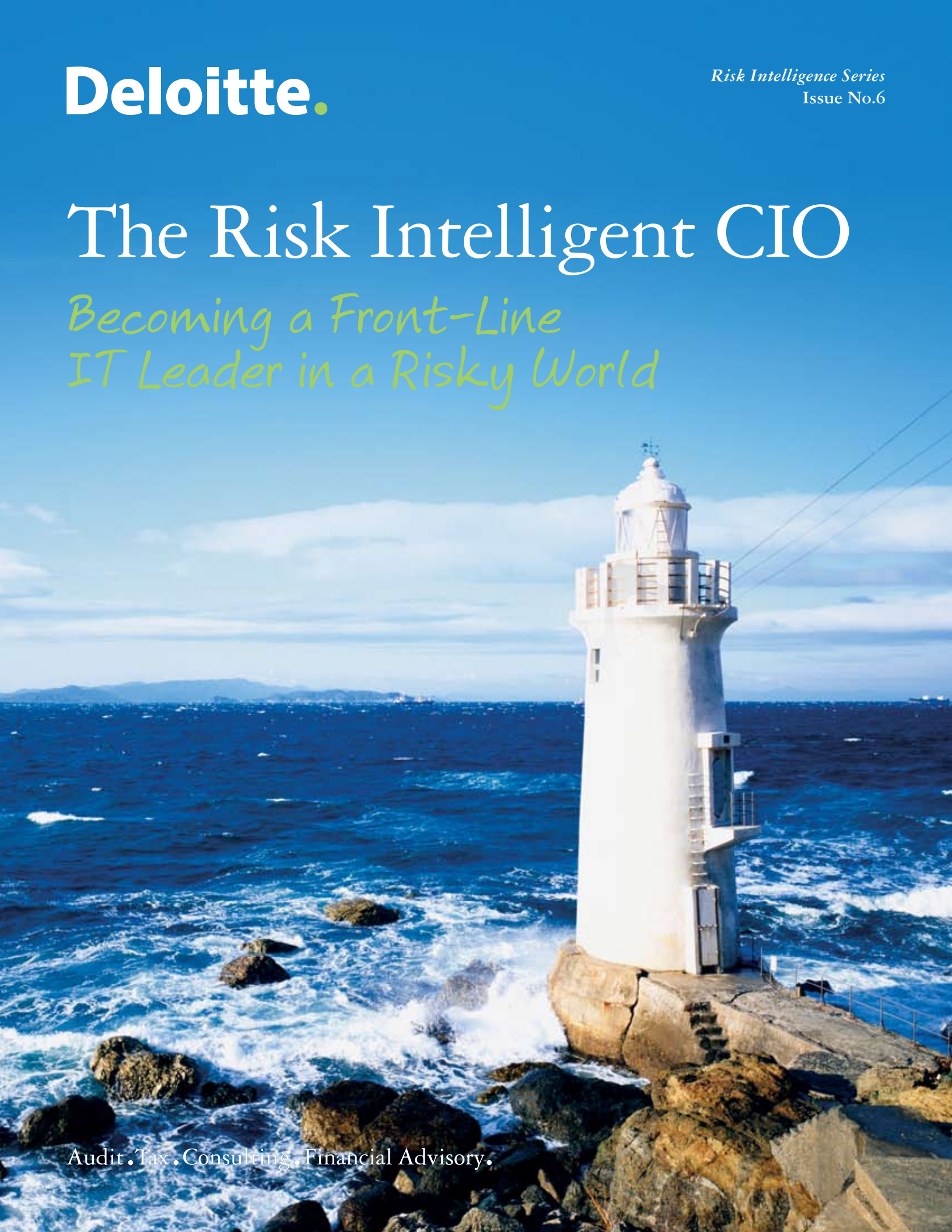
Deloitte.

Risk Intelligence Series
Issue No.6

The Risk Intelligent CIO

Becoming a Front-Line IT Leader in a Risky World



Audit . Tax . Consulting . Financial Advisory.

Table of Contents

Foreword

The publication represents the sixth installment in our series on Risk Intelligence. The concepts and viewpoints herein build upon those discussed in the first whitepaper in the series, *The Risk Intelligent Enterprise*™: *ERM Done Right*, as well as subsequent titles. You may access the previous whitepapers in the series free of charge at www.deloitte.com/RiskIntelligence.

Unfettered communication is a key characteristic of the Risk Intelligent Enterprise. We encourage you to share this whitepaper with the senior executive team at your company. The issues outlined herein will serve as a starting point for the crucial dialog on raising your company's Risk Intelligence while solidifying the important role of the chief information officer.

Preface

Imagine the benefits to your IT department, your entire organization, and your career if you:

- reduce the cost of regulatory compliance with a comprehensive approach to managing multiple and changing requirements
- increase the efficiency of risk management through automated controls and real-time monitoring of risks
- improve your organization's ability to prevent, detect, and correct critical risk issues with integrated systems and processes
- reduce the burden on business operations by helping coordinate existing risk management functions and eliminate redundancies
- enhance the quality of risk information by initiating or participating in an organization-wide effort to standardize risk management principles and language
- help improve strategic flexibility for mitigating risks to existing assets and for enhancing risk taking for reward
- provide a "comfort level" to the board, C-suite, and other stakeholders that the full range of IT-related risks is understood, monitored, and intelligently managed
- help to transform the culture into one that considers all decisions from a risk-based perspective
- initiate a process to document all risk decisions and associated trade-offs
- begin an initiative to document, integrate, and maintain various IT risk requirements in a single repository
- integrate and coordinate risk assessments, moving the organization towards a self assessment program to empower the business.

These accomplishments are all within the grasp of The Risk Intelligent CIO.

The Risk Intelligent CIO

Becoming a Front-Line IT Leader in a Risky World

In a business world as fraught with new risks as it is entwined with new technology, chief information officers (and those they report to) are increasingly aware that IT-related problems can come at a staggering cost to an organization's bottom line and reputation.

At the same time, perceptive CIOs realize that simply managing technology risks – however effectively they do so – is insufficient. Rather, they understand the imperative to exploit technology to manage risk across the *entire* enterprise, not merely within the IT department.

With heightened sensitivities around the issue of risk management, CIOs and IT professionals face both challenges and opportunities: to improve their IT department's risk practices; to elevate their role from low-profile caretaker to high-value leader; and to harness the power of technology across the organization to attain a higher level of risk management, operational excellence, and competitive advantage.

Grandiose goals for the IT shop? Far from it. Prescient CIOs already realize that information technology has a critical role to play in corporate governance, risk management, and regulatory compliance efforts. And they know that any organization-wide initiative should be tightly aligned with IT projects, priorities, and processes.

The current high-risk environment provides a unique transformational opportunity for IT leaders with the vision and ambition to grasp it.

The Anachronistic CIO

When technology was first making inroads into business, the IT leader's traditional job was "keeper of the infrastructure." The CIO-equivalent (the title did not exist at the time) presided over huge mainframes (and the requisite data punch cards), but little else.

Over time, as technology advanced into almost every aspect of the enterprise and became indispensable to the functioning of the organization, the CIO's profile began to rise.

If a single phrase could sum up the mission of technology executives during this phase, it might be this: "Get it done – better, faster, cheaper, and smarter." Their job was to support business processes and develop or deploy new applications. But they were rarely challenged on a managerial basis – they were "techs" more than "execs."

All in a Day's Work

The job description of today's chief information officer is more stressful and demanding than ever. CIOs face unrelenting pressure to:

- squeeze more productivity out of fewer resources
- deliver higher quality information within compressed timeframes
- drive down regulatory costs without jeopardizing compliance
- bolster system reliability and reduce downtime to an imperceptible fraction
- improve the satisfaction levels of internal customers
- reduce system and product complexity while dealing with vendors seemingly intent on providing the opposite
- initiate sustainable process improvements across the organization for competitive advantage, increased effectiveness, and reduced overhead.

CIOs of Eras Past

The evolution of the CIO has occurred at a rapid pace. Not so long ago, these three personality types dominated the landscape; today, they all hover near extinction.

The Guru
This CIO cultivates foresight. Considering himself a visionary, he views his role primarily as seer. Yet he doesn't suffer from self-delusion: others in the organization frequently share his view, and he often achieves a revered status. As for the day-to-day functioning of his department? The Guru doesn't have an operational bone in his body.

The Operations Guy
Deeply immersed in operations, this CIO can't see the motherboard for the circuits. What excites this IT leader is executing on service level objectives. If he pushes system availability from 99.7 to 99.8 percent, or if he attains his cost containment goals for the year, he considers it cause for celebration.

The Order-Taker
Part tinker, part soldier: blueprint in hand, the order-taker can build anything. Traditionally coming from an engineering background, this CIO spends much of his time down in the engine room, not up on the bridge. His mantra: "I'll build it for you – on time and under budget."

Likewise, their technology departments were basically miniature software companies. If traditional CIOs were unfamiliar with business strategy, it didn't much matter; the executive branch didn't understand IT either. Thus, technology and strategy were rarely uttered in the same breath.

The fortunes of the CIO took another turn ten-plus years ago with the rise of the Internet. Paradigms were being smashed and the World Wide Web was changing everything. CIOs seemed to be in a perfect position to become a true strategic partner in the business.

But somehow the opportunity slipped away. When the dot-com bubble burst in the first year of the 21st century, the aura surrounding CIOs was also punctured. Product and business organizations took over decision-making and strategy development around new technology tools, and CIOs once again became glorified caretakers responding to the needs of others.

Today, CIOs are pulled in many directions: by auditors, who want carefully documented evidence of strong IT controls; by CFOs, who want immaculate data, compressed closing cycles, and real-time information; and by CEOs, who want information upon which to base their strategic decisions.

Adding to the stress are recent trends in offshoring and outsourcing, which have broadened the CIO's responsibilities while simultaneously diminishing oversight capabilities; the rise in end-user computing, which has eliminated the relative safety of mainframe computing and replaced it with more-exposed user machines; and Sarbanes-Oxley, which has placed significant emphasis on general computer controls and has accelerated a shift away from manual and toward automated controls.

One might expect that with added responsibility comes added resources. Yet, despite all these new demands, CIOs frequently have trouble convincing executives about resource needs and work that needs to be done, often because CIOs tend to frame their arguments in technical terms.

The quandary for CIOs arose, we contend, because too many approached their job from a tactical perspective. Too often, IT leaders failed to look beyond the walls of IT. They frequently approached their work from a narrow, operational-delivery, compliance-based perspective. Activities were often project based, focusing on, say, regulatory compliance or fraud or network security, without considering the broader landscape.

Some CIOs were followers instead of leaders. Today, too many CIOs still run their departments according to the organizing principle: "I can do that; just give me a work plan." (There are, of course, notable exceptions of CIOs who have strategic responsibilities that are fully integrated into the broader business.)

The 21st Century CIO

Today, with the negative consequences of poor risk management escalating, CIOs are once again on the front lines. But while yesterday's problems usually had a monetary solution – companies could pay for a fix and move on – today's risks can't be managed just by throwing money at them.

The blows that a company can take to its brand and reputation (often followed by a hit to market capitalization) can stagger even the most resilient organization. Additionally, with changes in commercial law, and with organizations increasingly judged by negligence standards (a lower standard of proof under which defendants pay for harm caused by their unreasonable activity), today's CIO faces the grim prospect of fines or even incarceration for failure to live up to their expanded fiduciary duties or to stop a crime on their watch.

Saddled with greater responsibility than ever for the deeds (and misdeeds) of others, CIOs have no choice but to seize the moment and reinvent themselves. The role of "technologist" no longer suffices; today's CIOs are under pressure to become broad visionaries and develop risk management skill-sets outside their traditional domain. For CIOs who seek to become an integral part of the senior management team, opting out of this transformation is not a choice. The new expectations regarding corporate social responsibility and the intense regulatory environment will not allow it.

In this new world, CIOs need to understand various types of risk: risk inside their IT operation; risks facing the broader organization; risks in the use and deployment of technology; and strategic risk. Of these, the last is often the most neglected. Yet the task of leveraging technology to enhance strategic risk taking, of using technology to gather business information that can provide insights into the management of strategic risks, should rank among the most important.

Often, a lack of alignment between IT and the organization hampers the CIO's mission. Today's CIOs cannot allow that. They must establish IT priorities, processes, and projects to fully align with the needs and risks of the organization.

CIO's have essential knowledge and skills to help align IT and the rest of the organization, and to better coordinate IT assets with risk management needs. Boards, CEOs, and CFOs cannot do this without the CIO. Today's CIOs need to be leaders, not followers. In sum, they need to become "Risk Intelligent CIOs."

On Risk

We define risk as follows: *Risk is the potential for loss or the diminished opportunity for gain caused by factors that can adversely affect the achievement of an organization's objectives.*

Risk comes in many guises, providing both opportunity and peril. Poorly managed, it allows a security breach by a hacker or a disgruntled employee, exposing an organization to potential loss and liability. Effectively addressed, it provides infrastructure to support, for example, the treasury group in managing currency risk, or supports the chief audit executive by providing systems to aid internal audit.

Risks can have various levels of impact, and different risks can combine or interact to create new and greater risks. For example, as shown in recent news reports, a privacy risk (such as stolen customer databases) can quickly turn into a reputational risk, followed by litigation risk and financial risk, all in short order.

Risks can be characterized as "unrewarded" or "rewarded." Unrewarded risks usually bring no benefit to an organization. For example, risks affecting IT system availability, integrity of financial statements, and compliance with laws and regulations generally offer no reward even if they are properly managed.

Conversely, rewarded risk-taking can offer a benefit, sometimes substantial, to an organization. For example, well-managed risks associated with new technologies, products, markets, business models, alliances, and acquisitions can result in increased profitability and market capitalization.

Risk management is not solely a technology issue; there also exists a major people component. Behavior modification, reward and discipline, processes and routines, change management and training, and other personnel issues all come into play.

Today's increased reliance on technology has elevated associated risks to worrisome levels. Today, the consequences of disruptions are far worse and longer lasting than in decades past.

Similarly, increased supply chain integration, globalization of markets, and business cycle correlation present new risk challenges and demand better risk management practices to cope with shocks and disasters.

The Risky Life of the CIO

What risk factors face the CIO of the 21st century? Quite an array. Here's a partial list:

- increases in technology-related litigation and intellectual property lawsuits
- network security concerns around customer information and organizational secrets
- outsourcing and offshoring, which can provide important benefits but also carry significant risk
- expanding use of portable data devices, including laptops, flash drives, and other mobile technology
- proliferating computer viruses and related "malware"
- accelerating telecommuting trends
- greater dependence on third parties; increasing accountability for the mistakes (and even the crimes!) of others
- growing merger and acquisition activity
- government regulation, such as the Sarbanes-Oxley Act; numerous international, federal, and state privacy laws, such as the Health Insurance Portability and Accountability Act

The Risk Intelligent Enterprise

Despite a greater-than-ever need for effective enterprise risk management (ERM), confusion remains widespread in the workplace. This uncertainty is evidenced in the various approaches organizations take to ERM. In many cases, a senior executive will be nominally in charge of overall risk management, but he or she will quickly delegate responsibility and then exercise sporadic, or even negligible, oversight. In other instances, executives will respond reactively to new legislation, business initiatives, or events, rather than anticipating them and their associated risks.

Complicating matters, most C-suite executives don't really know what to expect of their IT groups in terms of managing risk, even as they shift major components of risk management execution to IT with vague instructions to "take care of it."

For their part, many CIOs are familiar with risk management as it pertains to their operational and security risks. But too many CIOs have segmented skill sets. Responsible for running the IT system, many still focus mainly on operational risks and data security to the exclusion of broader threats. Yet the situation facing CIOs calls for a radically different approach, because organizations today face risks that are unprecedented in corporate history.[1]

The term "Risk Intelligent Enterprise" describes organizations that have attained the highest state of risk management. Many characteristics define such enterprises, but for the purposes of this paper, we'll address just a few. (For a deeper discussion, see "The Risk Intelligent Enterprise: ERM Done Right" and other whitepapers in the Risk Intelligence series.[2])

Bridging Silos: Risk Intelligent Enterprises not only nurture risk expertise within their divisions, departments, and units, but also carefully build bridges between these risk "silos" to open lines of communication, share information, consider risk scenarios and the interaction of multiple risks, and gain a broader perspective on the totality of risk. Part of the bridging process includes developing common risk terminology and metrics so that everyone in the organization "speaks the same language."

Assessing Impact: With today's enterprises facing a seemingly infinite number of risks, it's impractical – if not futile – to attempt to plan for every single one. Thus, CIOs should focus on the finite impacts that could result from myriad threats. A business impact analysis can help illuminate the ways that an organization can be affected, regardless of the cause. For example, instead of having separate contingency plans for hurricanes, terrorist attacks, brownouts, fire, and sabotage (infinite causes), create a plan to address the impact of network unavailability (finite impact).

Risk Taking for Reward: Risk Intelligent Enterprises operate under a philosophy that encompasses not only risk mitigation, but also risk taking as a means to value creation. Risk taking for reward can assume many forms, from strategic acquisitions to research and development to entering new markets. Some organizations establish shared services centers to reduce the risk of numerous entities handling similar processes in a divergent manner; others take it a step further and use their shared services center as a platform to offer third-party services to other companies, turning a cost center into a revenue center in the process.

In our experience, organizations that are most effective and efficient in managing risks to both existing assets *and* to future growth will, in the long run, outperform those that are less so. Simply put, companies make money by taking intelligent risks and lose money by failing to manage risk intelligently.

1 Colvin, Geoffrey, "Managing in Chaos," *FORTUNE*, October 2, 2006. This study of S&P 500 companies showed that overall risk levels more than doubled between 1985 and 2006. In 1985, only 35 percent of the S&P 500 faced high risk and highly volatile long-term earnings growth. By 2006, that number had risen to 71 percent. During the same period, the number of companies enjoying low risk and volatility fell from 41 percent to 13 percent.

2 www.deloitte.com/RiskIntelligence

The Risk Intelligent CIO

How do Risk Intelligent CIOs fit into this picture? By thinking expansively about how to tap into the potential of technology to intelligently manage risk.

This means, among other things, identifying the right people to manage risk and providing them with appropriate training. It also involves championing a risk management philosophy that includes intelligent risk-taking for reward as well as risk mitigation.

Overall, the Risk Intelligent CIO must harness technology to embed risk management into the organization's day-to-day operations. Today's enlightened CIOs work to instill a common language to talk about risk and common metrics to measure it. They strive to unite risk management and monitoring initiatives across the corporate culture, instead of relying on separate processes for separate departments or organizational silos. They work in active partnership with other CxOs and executives in the organization's business, risk, finance, and other functions to accomplish all of the above through collaboration, consensus building, and teamwork.

In organizations that have established a risk committee, the CIO can help improve the decision-making capabilities of that group by providing timely access to relevant information; by facilitating an enterprise-wide view of risk; and by harmonizing the various risk issues the business units are dealing with, such as regulatory compliance.

The CIO's role entails both give and take. The manner in which the technology organization manages risk should be consistent with the approaches established by the central risk function. But at the same time, the CIO's group should provide infrastructure and support for technology platforms to measure and monitor other risks for the organization at large.

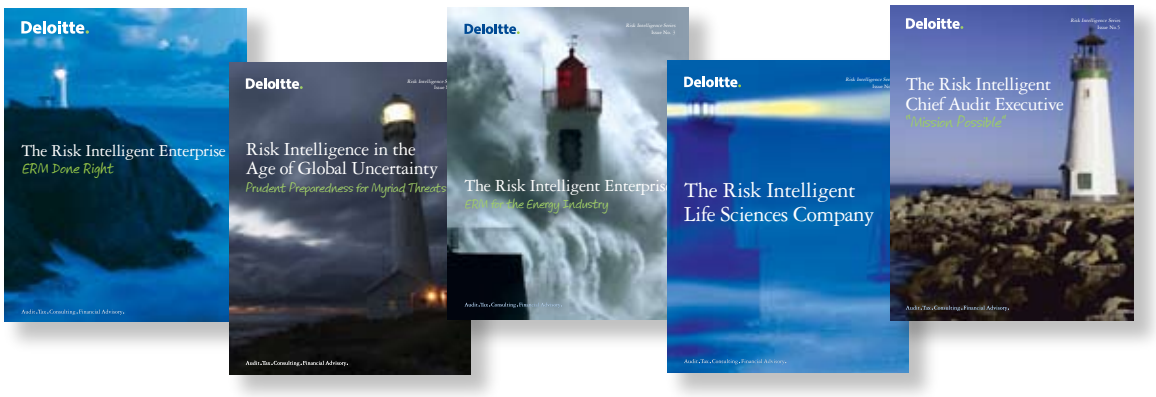
Of course, for today's CIO, managing risk isn't merely about technology solutions – it's about management and leadership. CIOs have to change, either personally, by adapting to the new realities, or institutionally, by being retired, replaced, or redeployed.

A Risk Intelligent CIO devotes attention and resources to the following:

- the risk management processes that apply to the IT department – identifying, assessing, managing, and reporting IT-specific risks such as security, privacy, and business continuity
- the application of technology infrastructure across the enterprise to help other groups identify, assess, manage, and report *their* risks
- playing a true executive role in understanding how it all comes together at the enterprise level, ensuring that strategic risks are considered appropriately, and helping the board understand an enterprise's risks and the corresponding action plans that they need to be aware of.

Is Your Company Risk Intelligent?

See our full series of whitepapers on Risk Intelligence, including the following:



No. 1: *The Risk Intelligent Enterprise: ERM Done Right*

No. 2: *Risk Intelligence in the Age of Global Uncertainty*

No. 3: *The Risk Intelligent Enterprise: ERM for the Energy Industry*

No. 4: *The Risk Intelligent Life Sciences Company*

No. 5: *The Risk Intelligent Chief Audit Executive*

Visit www.deloittte.com/RiskIntelligence to download electronic copies, or contact your Deloitte professional for print copies. There is no charge for these publications.

The Risk Intelligent CIO: Self-Assessment Quiz

Take this test to determine your Risk Intelligence. Score 1 point for "yes" answers; 0 points for "no."

Do You … ?

1. Recognize (and strive to influence) your enterprise's highest strategic priorities?	☐ Yes	☐ No
2. Understand IT's role in the organization as a whole?	☐ Yes	☐ No
3. Help develop an integrated view of the risks facing the entire organization, not solely the IT department?	☐ Yes	☐ No
4. Assess how prepared your organization's systems are to withstand different types of risks and impacts, and develop ways to improve that resiliency?	☐ Yes	☐ No
5. Understand the relevant laws and regulations your company needs to comply with?	☐ Yes	☐ No
6. Align IT assets with compliance priorities?	☐ Yes	☐ No
7. Check for any untapped potential, redundancies, or needless complexities in existing systems caused by the traditional fragmented organizational structure?	☐ Yes	☐ No
8. Know what your peers within and outside your industry are doing in terms of innovative risk management practices?	☐ Yes	☐ No
9. Focus on reducing regulatory compliance costs through automation, standardization, and consolidation?	☐ Yes	☐ No
10. Continually improve your organization's capabilities to develop, produce, and deliver information with better solutions, processes, and systems?	☐ Yes	☐ No
11. Believe that if you could design your risk management program from the ground up, you would still do things the same way you are doing now?	☐ Yes	☐ No
12. Know how much risk management is costing your organization today? Have you projected costs for the quarters and years ahead?	☐ Yes	☐ No
13. Know how to measure the return on your investment in integrated risk management organization-wide?	☐ Yes	☐ No
14. Know how to make the case that the return on investment justifies the cost?	☐ Yes	☐ No
15. Know the drivers and timelines of future risk?	☐ Yes	☐ No

Scoring

14-15 points: Your Risk Intelligence borders on genius!
10-13 points: Your risk smarts are in the upper echelon, but a little more study couldn't hurt.
6-9 points: You are smack in the middle of the pack. More schooling needed.
0-5 points: Your organization is at risk, and you need to be part of the solution. Immediate remedial work required!

The Stuff of CIO Nightmares

It may be clichéd to ask, "What keeps you awake at night?" Yet for many CIOs, sleepless at 2 a.m., the question carries a disquieting relevance. Highly publicized cases revealing IT insecurity can embarrass the organization, provoke disruptive lawsuits, and threaten careers. The loss of privileged information, security breaches, and other threats have become the stuff of CIO nightmares. These cases illustrate the need for new priorities for the CIO, who must do a better job of explaining to CEOs how these risks fit into the company's strategic picture.

Weak technology planning can also provoke insomnia in CIOs. Failed technology investments, delayed system improvements, premature retirement of existing technology, and other occupational blunders can all lead to significant negative consequences, and can hit the bottom line with substantial unnecessary costs.

Even job stability is no longer on the even keel it once was for CIOs. Amid heightened expectations from CEOs and boards, and concerns that IT is not fully meeting the demands of risk management, some organizations have been shuffling the organizational chart.

Recent studies place the average tenure of CIOs at two years, an improvement over the 18-month turnover rate of a decade prior, but hardly a model of stability.

Anecdotal evidence suggests that many CIOs are being replaced by non-technical people coming from outside IT, such as executives in the HR and financial organizations. At a time of increasing IT complexity and cost, why would a "non-techie" be named CIO? Because senior executives and boards recognize that cost and complexity are no longer their most pervasive issues; they are worried about the bigger issues of corporate governance, risk management, and regulatory compliance. These problems are not the traditional province of CIOs, and some new non-technologists thrust into the CIO role are thought to have a broader view of the organization and the risks it faces.

In this climate, harried CIOs must continually prove their worth. Many will find themselves asking, "What does risk management mean to my department? How can I make it work? How can we use technology to manage risk for the whole enterprise?"

The Role of CROs and CTOs

The rise of information technology and its use in managing risk has spawned some new corporate positions while enhancing others.

The chief information officer (CIO) is a managerial executive charged with organization-wide responsibility for information technology. This job's importance has increased dramatically in recent years with the growing reliance of business on IT. More recently, the job's cachet – and challenges – have grown as IT is harnessed to manage risk. Sometimes, the CIO becomes an executive board-member. More typically, the CIO reports to the CEO or CFO.

The chief risk officer (CRO) is a relatively new post aimed largely at helping organizations limit their exposure to risk and liability. The position, which emerged in the wake of new laws and government regulations, focuses largely on compliance. But as more large organizations create CRO positions, the CRO's role has been expanding to help the CIO accomplish other key risk-management goals.

The chief technology officer or chief technical officer (CTO) is a corporate business executive whose position emerged in large research-driven companies back in the 1980s as a business extension of the R&D director's job. The CTO focuses mainly on technology, coordinating technology with business strategies and launching various technology initiatives.

Although significant variance exists, in most companies that have all three titles, the CIO ranks as most senior. But regardless of their relative positions on the organizational chart, these three executives should work collaboratively toward their shared risk management objectives. Each should make sure that their technology and operational risks are properly and consistently managed within the larger framework. And the CIO and CTO should work with the CRO to provide support and infrastructure for risk management activities across the organization.

The Evolving Role of the CIO

CIOs typically have a good handle on their departments and the risks associated with that slice of the business. But rare is the CIO who has used technology as a fulcrum and their role as a lever to help manage the broader risks faced by the organization.

To succeed in the 21st century, CIOs need this broader view. For many, the challenge will involve breaking down the walls between the functional business units. Implementing organization-wide solutions requires substantial consensus building and buy-in; as a result, the skills the CIO must bring to bear will often be of a diplomatic nature.

Other CIOs will need to first knock on doors before they can break down walls. That is, they need to gain entrance to the C-suite instead of remaining cloistered in the IT environment. Such a move may give rise to questions in the mind of the CIO: "What do I need to focus on first? What do I need to do differently? How does this align with the day-to-day departmental operations? What could I be doing better right now?"

> **Rare is the CIO who has used technology as a fulcrum and their role as a lever to help manage the broader risks faced by the organization.**

To start this journey, the Risk Intelligent CIO should envision the role as evolving from that of guardian of all things IT to a more thoughtful, strategic position exploiting technology to support the whole enterprise. This IT leader should perceive this new mandate as multifaceted and strategically critical.

Launching CIOs on the path to Risk Intelligence will also require IT-savvy boards. Increasingly, boards are recognizing their own need to become more technology-literate so they can have a deeper understanding of risk and ask tougher questions about it. This may be driven in part by recent New York Stock Exchange requirements that the board be regularly informed of the company's risk management practices. This is a positive development. The Risk Intelligent CIO welcomes an engaged, IT-savvy board.

Meanwhile, the CIO must wear several hats as a cross-functional leader, providing guidance to the whole organization about integrating IT across the entire enterprise to meet regulatory compliance requirements and mitigate other risks. The CIO should outline the business case for integrating risk management more comprehensively into the organization.

This means the Risk Intelligent CIO should understand the risks the business faces, and stand ready to offer advice on IT projects and larger business strategies, considering the technology requirements and related risk management issues. Identifying risks to the organization means looking at the impact of risk as well as sources of risk. It means making a comparative analysis of publicly disclosed risks, investigating an organization's prior risk experience, and performing a business impact analysis of critical assets.

Not only can CIOs raise issues, they can do such things as explore hiring additional risk specialists; investigate different ways of running things, such as changing the system development lifecycle; and look at risk implications in every area, from strategy to applications development, infrastructure, and security.

In doing this, the goal of the Risk Intelligent CIO should be to help move the organization from a fragmented organizational model to an integrated structure with risk management embedded in it. This means identifying core processes and enabling technologies that lend themselves to integration, and evaluating risk according to common criteria. Instead of evaluating the risk for each silo, it means providing a common risk assessment approach and tying risk management back to the organization's broader risk planning strategy. It also means working to change the corporate culture, and making sure information moves through the whole organization, including operations, compliance, and risk, using a common language.

Of course, the CIO, no matter how talented, can't accomplish all of this single-handedly – clearly a team effort is called for. But the CIO can assume an essential role on that team. Two tasks, in particular, require the CIO's skill set: (1) applying the assessment criteria to the IT-specific risks for which the CIO is responsible; and (2) providing the harmonizing, enabling technology for everyone else to use.

An IT Risk Management Success Story

One example of successful risk management integration involves a complex, global organization with millions of customer accounts in scores of countries. For several years, the company pursued an aggressive growth-through-acquisition strategy, which seemed like a roaring success story … except that the organization had more than 300,000 employees around the world, thousands of servers and applications, a petabyte of data, and a monumental regulatory compliance challenge.

To confront the challenge, the company launched a risk management initiative – consistent with our definition of Risk Intelligence – and a standardized risk management system throughout its global IT enterprise. This new system included five major building blocks:

- a standards-based risk management methodology that was carefully aligned with other standardization efforts across the entire company
- an enhanced and integrated risk and control self-assessment process that accommodated a host of relevant regulatory requirements and assessment methodologies, including FDICIA[3], GLBA[4], SOX 404[5], and Basel II[6]
- a workflow management system that provided a single platform for managing the risk assessment execution and reporting
- a global rollout that melded operations across seven operating regions with the new system
- a global compliance and risk management office, redesigned to manage the new process.

As a result of these efforts, this global behemoth was able to demonstrate substantial benefits. These included:

- reduced complexity – the company significantly reduced the number of reporting entities
- consistent risk and controls – the company reduced tens of risk profiles per domain to one risk profile per domain
- tool-enabled workflow – the company went from hundreds of hours using spreadsheets to tens of hours leveraging a database and common data definitions
- streamlined reporting – the company improved from no trending and slow reporting to trending capabilities and rapid reporting
- improved sampling – the organization went from 100 percent control testing to country-level sampling
- Basel II support – the company moved from limited to advanced capability
- traceable requirements – the company evolved from best practices "piling on" to a single set of authoritative sources linked to defined control objectives
- most significant of all, the company demonstrated the type of operational agility usually known only to early-stage, entrepreneurial start-ups.

Key Recommendations

In our experience, the most successful CIOs don't limit their attention to the IT department. Rather, they approach their position as that of a true C-suite executive, one concerned with the strategic and operational issues facing the organization as a whole. These CIOs embrace innovation and change as they develop and manage their Risk Intelligent IT programs. Listed here are some key considerations to start the journey:

Take small steps: Before you expand your attention to the overall organization, an important first step is to assess your department's current state of risk management. How costly is your existing risk management process? Are the people involved with risk management efforts satisfied with existing processes? How and where are complications and frustrations surfacing? Do you know your department's risk profile (or tolerance for risk)? How does that synch up with your organization's overall risk profile? Which capabilities or solutions need to be improved or procured?

Prioritize based on impact: After determining the department's risk management maturity level, begin to prioritize by focusing on the most attainable initiatives with the highest business impact (in business jargon, the "low-hanging fruit"). Performing a business impact analysis can help shed light on the areas (or vulnerabilities) that have the potential to generate business benefits and lead to greater preparedness for the organization.

Automate controls: The imperative to rein in compliance costs provides CIOs with a fresh and crucial opportunity to convince management of the merits of automation and consolidation. Arguments that highlight the benefits of a single system, fewer errors, and easier testing and verification, coupled with the potential to dramatically lower expense, should prove compelling.

3 Federal Deposit Insurance Corporation Improvement Act of 1991

4 Gramm-Leach-Bliley Act of 1999

5 Section 404 of the Sarbanes-Oxley Act of 2002

6 The second of the Basel Accords, which are recommendations on banking laws and regulations issued by the Basel Committee on Banking Supervision.

Assign user profiles that reflect roles and responsibilities: Develop and customize system profiles for employees and executives that can return the appropriate level of information for their roles. This feature allows the business to have better control over user access. It also allows the efficient delivery of relevant information to those making business decisions.

Improve information governance: Bridging the gap between technology and governance, risk, and compliance initiatives leads to better risk management and improved performance. Examine the IT strategies, policies, procedures, architectures, and technologies necessary to meet your organization's information needs. To overcome the resistance that often accompanies efforts to improve information quality, consider using a "soft" tactic – deploying tools to monitor data quality behind the scenes.

Align IT assets with broader risk management needs: Most CIOs have a handle on the risks facing their unit, but only a few may be aware of those facing the organization at large. Those CIOs with narrower perspectives should get up to speed on the risk needs of the organization and work with other unit leaders to devise the most efficient and effective IT response to meet those needs.

Apply lessons learned: In the dash to meet Sarbanes-Oxley requirements, many companies added tactical and redundant processes and controls. Now that several years have passed, it's time to weed out complexity and redundancy and simplify controls. But don't stop there: Extend the housecleaning to operational and regulatory processes.

Start With Simple Tasks

- Find a way to interject the subject of risk into all your conversations.
- Help to align risk terminology and metrics across organizational "silos," so that everyone is speaking the same language.
- Understand your current capability (or lack thereof) to manage risks.
- Identify your most material risks.
- Meet as an executive team to discus what should be done with these material risks.
- Establish a straightforward, standard risk reporting template for leadership.
- Dedicate resources to risks that have a high chance of return on investment.
- Share internal risk management knowledge with risk owners assigned to more complicated risks.
- Incorporate risk identification, assessment, and analysis findings into yearly decision-making processes.

The Risk of Bad Information

Information management represents a particular area of need (and thus, for CIOs, opportunity). Despite billions of dollars in technology investments, more than 60 percent of executives in a global study of information quality still reported that the accuracy, timeliness, and availability of financial information was lacking, according to "IQ Matters," a report by CFO Research Services and Deloitte Consulting LLP. More than 80 percent felt information about performance and risk management failed to meet their objectives.

IT professionals are uniquely qualified and positioned to help deliver high-quality information. By forging relationships with the business side of an organization, developing plans to simplify and integrate disparate processes and systems, and building IT capabilities necessary to increase *Risk Intelligence*, CIOs can play a prominent strategic role in achieving performance and risk management goals.

Becoming a Risk Intelligent CIO

The increasing need to effectively manage risk should compel IT leaders to redefine their role – to one that is more creative, proactive, innovative, and strategic than ever before. As the executive team seeks guidance for increasingly complex corporate governance, risk management, and regulatory compliance issues, the CIO must have a seat at the table. This elevated role requires a deeper and broader perspective on how IT can evolve from its conventional duties of protecting enterprise assets into a new, more strategic responsibility of creating value and enhancing the competitiveness of the organization. In doing so, CIOs will improve the fortunes of the entire enterprise, those of their IT department, as well as their own professional growth and advancement.

IT can evolve from its conventional duties of protecting enterprise assets into a new, more strategic responsibility of creating value and enhancing the competitiveness of the organization.

Appendix

10 Key Steps to Risk Intelligence

Strategic

1. Drive the principles of intelligent risk management from the top down and embed it into the culture of the organization.

Risk Identification

2. Link risk directly to value creation and strategic initiatives.

Risk Assessment

3. Leverage probabilities when appropriate, but consider your vulnerabilities when assessing the risk of unique or unknowable events.
4. Recognize how quickly risk situations can accelerate in the age of the Internet and global communication.
5. Improve the accuracy of assessing and measuring loss of value (opportunities missed due to unanticipated or poorly managed risk).
6. Identify and address the root causes of failure: people, processes, systems, external factors.

Risk Response

7. Prepare appropriately for finite, relevant, high-impact events.

Design and Test Controls

8. Harmonize (ensure risk managers all speak the same language), synchronize (coordinate across institutional boundaries), and rationalize (eliminate duplication of effort) risk management requirements.

Monitoring and Assurance

9. Leverage internal audit to gain independent assurance that appropriate mitigating processes are in place.

Sustainable Capability

10. Identify and close gaps in required capabilities in a timely manner.

Contacts:

Mark Layton
Global Leader
Enterprise Risk Services
Deloitte & Touche LLP
214-840-7979
mlayton@deloitte.com

Adel Melek, MSc., CISSP, CISA, CPA
Partner
Global Leader – Security & Privacy Services
Deloitte & Touche LLP
416-601-6524
amelek@deloitte.ca

Chris Lee
National Managing Partner
Security & Privacy Services
Deloitte & Touche LLP
408-704-4314
chrislee@deloitte.com

Lee Dittmar
Principal
Deloitte Consulting LLP
215-446-3692
ldittmar@deloitte.com

Robert G. Hansen
Principal
Global Leader, Control Assurance
Deloitte & Touche LLP
203-708-4256
bohansen@deloitte.com

Edward Hida
Partner, Capital Markets
Risk Advisory Service Line Leader
Deloitte & Touche LLP
212-436-4854
ehida@deloitte.com

Ken Landis
Principal
U.S. Co-Lead, Technology Advisory Services
Deloitte Consulting LLP
212-618-4800
klandis@deloitte.com

Bill Kobel
Principal, Enterprise Risk Services
Deloitte & Touche LLP
214-840-7120
bkobel@deloitte.com

Philip Baltunis
Director
Deloitte & Touche LLP
212-436-6296
pbaltunis@deloitte.com

Acknowledgements:

The following made significant contributions to the development of this publication:

Philip Baltunis
Paul Barbour
Mark Baylis
Jack Burlingame
Lee Dittmar
Robert G. Hansen
Edward Hida
Matt Hourin
Bill Kobel
Ken Landis
Mark Layton
Chris Lee
Adel Melek
Terrie Perella
Kristy Ragones

#7188