



IT risk management: Balanced maturity can yield big results



Brian Barnier, strategy, governance and risk, CIO Office, IBM
Dr. George Westerman, research scientist, Center for Information Systems Research, MIT
Sloan School of Management

January 2009



Contents

- 2 Highlighting a more effective approach to IT risk management
- 3 Meeting heightened concerns
- 5 Leveraging the benefits of maturity on the three core disciplines
- 8 Framing IT risk management discussions
- 10 Linking IT risk management with IT and business performance
- 12 How does your organization measure up?
- 15 Conclusion

Highlighting a more effective approach to IT risk management

Think IT risk management is just about spending money to avoid risks? Think again. Recent research shows that organizations taking a balanced approach to IT risk management maturity have fewer incidents—but also stronger overall IT and business performance—than their competitors. Note the emphasis on the term “balanced.” An organization might gather volumes of IT risk management data, for example, but not be able to organize and act on that data. It may have a very well-designed and managed technology foundation but may suffer failures because of poor user risk awareness. Or it might focus on IT governance processes without addressing the culture or technology foundation in which governance operates.

Organizations with balanced risk management maturity not only avoid disruptions to the business but also tend to have better IT performance in areas such as managing costs and supporting change in the business. Instead of just addressing the risk of the day, CIOs can use risk management to make the case for better IT management practices. This white paper is about how CIOs can improve their IT risk management outcomes *and* gain a variety of business and professional benefits.

Now is the time to balance maturity across the three risk management disciplines.

Meeting heightened concerns

A 2008 survey on IT risk management conducted jointly by IBM and MIT Sloan School of Management's Center for Information Systems Research (MIT CISR) shows that excellence in one IT risk management area delivers only part of the possible payoff from risk management. It points to a far more effective approach that balances the three core IT risk management disciplines:

- Risk governance process—risk-related policies combined with a consistent process to identify, prioritize, address and monitor risks over time
- IT foundation—IT infrastructures and applications that are well architected and well managed
- Risk-aware culture—IT and business staff members who are aware of threats and risk-related policies and have a culture that encourages discussions about risk

This survey builds on previous research by George Westerman and Richard Hunter, as presented in their book *IT Risk: Turning Business Threats into Competitive Advantage*.¹

The survey also underscores the growing importance of IT risk management in most enterprises. More than half of risk managers surveyed report that concern about IT risk has increased in their organizations over the last year, as opposed to just 8 percent who say it has decreased. This echoes the IT Governance Institute's *IT Governance Global Status Report—2008*, which shows that 62 percent of respondents have already implemented or are now implementing IT risk management measures, compared with 45 percent in 2005 and only 18 percent in 2003.² What's more, executives in the IBM/MIT CISR survey report that they are trying to manage risk differently, with 79 percent actively launching a more unified IT risk management effort than before.

IBM and MIT CISR 2008 IT risk management survey

- Telephone interviews with 258 senior line-of-business (LOB) and IT executives and managers during June and July 2008
 - United States and Canada: 50 LOB and 28 IT
 - France: 36 LOB and 24 IT
 - United Kingdom: 32 LOB and 28 IT
 - Australia and New Zealand: 40 LOB and 20 IT
- Company sizes: 1,000+ employees
- Industries: 18

This reflects several business environment factors: mergers and acquisitions, increased IT risk resulting from greater IT complexity, higher costs of IT risk incidents, and the almost universal need to lower costs. Much of this is driven by the tight coupling of IT with the global business environment, which increases vulnerability to events around the world. In addition, the need for compliance with an increasing number of industry standards, regulations and contractual requirements is driving action. According to survey results, regulatory requirements and policy mandates are bigger drivers of unified risk management efforts than adverse events. Additional drivers mentioned in the survey include senior executive changes and requirements involving contracts, industry issues and supply chains.

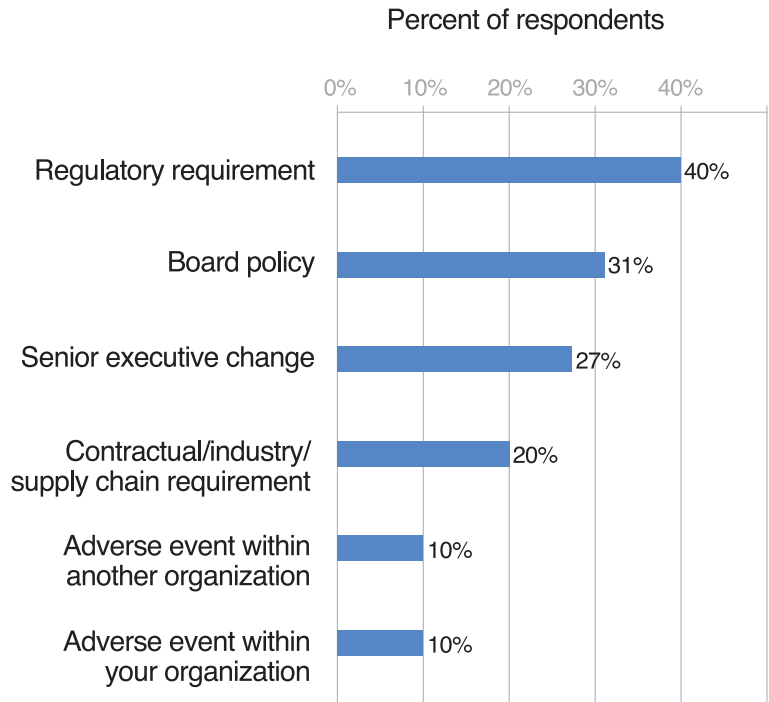


Figure 1
Survey respondents rated these reasons for launching a more unified risk management effort.

IT risk governance, IT foundation and a risk-aware culture can address risk management issues.

Survey respondents reported that the greatest barriers to effective risk management are a lack of awareness along with the lack of a trained staff and the tools necessary to deal with threats. The good news is that the three core disciplines—risk governance process, IT foundation and risk-aware culture—can address these issues. However, survey results show that many organizations have a long way to go in accomplishing this. Although risk managers report some capability on all three disciplines, they are not as mature as they can or should be.

Leveraging the benefits of maturity on the three core disciplines

According to the IBM/MIT CISR survey, organizations that have balanced their maturity across all three of the core risk management disciplines—instead of letting one outpace the others—are more effective in managing risks. They report greater IT effectiveness than organizations with a less unified approach in the following areas:

- Ability to avoid negative incidents such as outages and security leaks
- Efficiency of the IT unit
- IT and business alignment
- Ability to support business changes

In addition, organizations with a balanced risk management approach report more favorable perceptions of IT risk management capability than those that do not employ all three disciplines. Just 10 percent of out-of-balance organizations say that IT risks are effectively managed by their companies, while 72 percent of organizations with balanced maturity make that claim. Furthermore, organizations with balanced maturity report higher levels of success in managing their most important IT risks.

While risk governance processes are more important initially, the IT foundation and a risk-aware culture become important later.

Although prior research has suggested that all three IT risk management disciplines are important, the IBM/MIT CISR survey goes a step further. It shows that risk governance processes provide different value than the IT foundation and risk-aware culture. The risk governance process—gathering information on risks and ensuring that they are being managed—is essential for getting and increasing stakeholder confidence in risk management. It helps the board and senior executives understand what risks the organization faces and ensure that the right actions are taken in both investment selection and implementation. Companies with good risk governance processes were more effective at managing all IT risks. However, the relative importance of risk governance processes lessened as businesses became more mature in terms of the IT foundation and a risk-aware culture.

Although maturity of the IT foundation and a risk-aware culture are much harder to achieve than risk governance processes, they are more closely associated with IT performance. Organizations that are more mature in these two disciplines report higher levels of efficiency, agility and value from IT, along with lower risk. The goal, then, is to use the risk governance process to gather information and get attention for risk management and then use that attention to bake risk management into everything the company does. In short, meaningful governance seems to jump-start a balanced risk management process. Using risk management to actually improve the IT foundation and risk-aware culture yields more powerful benefits than just bolting additional protections onto a shaky IT foundation or a risk-unaware culture.



Risk management approaches can help mitigate IT risk while also helping to improve IT management processes.

To better understand how this operates in practice, consider what organizations employing the various industry risk management practices have learned. The most widely applied approaches are derived from the IT Governance Institute's Control Objectives for Information and related Technology (COBIT) approach, from quality control approaches such as ISO 9000 or from IT management frameworks such as IT Infrastructure Library® (ITIL®) standards. While these approaches can be helpful in managing IT risk, they also provide guidance on building IT risk into governance processes for portfolio management and investment allocation. In other words, they start to help improve IT management processes, not just make IT less risky.

One point from this survey is that although a strong risk governance process is a starting point, it is not enough. Risk governance is a bit like a maintenance manual that says what should be done and when to do it. The real benefit comes from being aware of the instructions and taking action. Similarly, organizations can use risk governance to improve the IT foundation and build a risk-aware culture to achieve a balanced approach. Organizations with a balanced approach can use their risk governance process to get attention for bigger changes in IT management. They can improve the IT foundation by removing complexity and improving infrastructure management controls and processes—instead of just patching holes or understanding weaknesses. They can build awareness activities and communication practices around the risks they see as most important, reinforcing a culture that is risk aware and pulls together to solve the risks that arise. That perhaps explains why companies in the top third of risk maturity report 28 percent higher business agility than other companies in the survey.

Frameworks like COBIT and Val IT can provide good ways to help ensure that the IT foundation is managed to achieve the desired results by using intentional, risk-aware, continual improvement processes to drive expected outcomes.

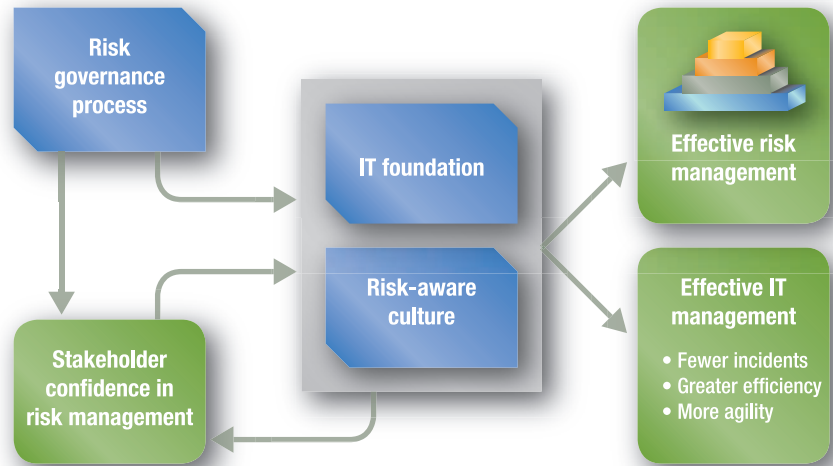


Figure 2
This diagram shows how the three disciplines can improve risk management and IT management.

CIOs can facilitate discussions about IT risk with business executives by using the four A's.

Framing IT risk management discussions

The most important way to start improving risk management is to find a shared language that IT and business executives can use to discuss IT risks. The Westerman-Hunter book identifies a framework of “four A’s” that serves this purpose very effectively:

- Availability—keeping existing processes running and recovering from interruptions, while avoiding negative incidents such as outages and security leaks
- Access—ensuring that the right people have access to appropriate information and that the wrong people do not
- Accuracy—providing accurate, timely and complete information to all relevant stakeholders
- Agility—supporting changes in the business with acceptable cost and speed³

Discussions around the four A's can help clarify how much risk is too much—and too little.

The four A's



SOURCE: George Westerman and Richard Hunter, *IT Risk: Turning Business Threats into Competitive Advantage*, Harvard Business School Press, 2007, 57.

Figure 3

The four A's put IT risks and their causes into language that business executives can understand. Because the causes of all four A's are interdependent, discussing them also helps remove the perceived contradiction between agility and availability or access risks. Working from the bottom to the top of the pyramid is a useful way to address risk that aligns with organizational responsibilities and risk factors.

It is interesting to note that IT and LOB risk managers have different perceptions of IT risk. LOB risk managers in the survey attach more importance to accuracy and agility than IT managers do. They also view their IT risk management capabilities as more mature than IT risk managers do. Perceptions of IT risk management also vary by country and industry.

These different perceptions can provide an opportunity for discussion. In fact, one of the most important starting points is a discussion among different stakeholders on how effective their organization is on each of the four A's, how current practices

can get in the way of managing some risks and what can be done to not only reduce risk but also improve performance. These discussions usually clarify just how much agility risk is too much (or too little), how much protection each business process really needs for availability risk and so forth.

Linking IT risk management with IT and business performance

Effective IT risk management is not about technology—it's about management.

The good news from the survey is that IT risk management doesn't have to be just a cost of doing business or a drain on business speed and flexibility. The fact is, IT risk management is not a technical issue. It is a management issue. Effective IT risk management is really about improving the way the company manages its IT. By building balanced maturity across the three core disciplines, organizations can turn IT risk issues into improvements throughout IT and the business.

IT risk did not originate from IT practices alone. Although some risks arise from an organization's business environment, most risks arise internally from the trade-offs—and sometimes mistakes—organizations make in allocating funds, building systems and managing people. Every decision to grant an exception to a standard, to buy from an unproven vendor, or to shortcut steps in the system development and testing process creates potential risk conditions. Sometimes the trade-off is worth it; many times it is not. Both IT and business executives must be involved in improving IT risk management and consider risk when making other IT decisions. To facilitate this, it's vital to find a language that both parties can use to discuss risk, such as the four A's: availability, access, accuracy and agility.

Discussions about IT risk should be more about a balanced risk management capability and less about technology.

CIOs can use IT risk management to help make the case for good IT management practices that may not always have a quantifiable ROI, such as architectures and project methodology. They can get LOB attention by placing IT discussions in the context of risk and return issues that matter to the business. Discussions based on the four A's and a balanced risk management capability—as opposed to discussions about technology, hacking techniques and complex mathematical distributions—are more effective with the typical business executive because they are about business decisions rather than technical jargon.

The results of this new IBM/MIT CISR survey show that CIOs can put IT risk management at the forefront of their discussions with the business, which can draw business and IT together. Many business decisions involve fundamental trade-offs about IT risk—not just return—including:

- Integrating acquired companies
- Purchasing software as a service
- Investing in application enhancements
- Outsourcing and offshoring
- Integrating diverse applications
- Ensuring compliance
- Finding the right level of availability and access protection.

Considering an initiative's effect on risk as well as return allows IT and business managers to make better decisions now and for the future.

CIOs can get started by rating their organization's balance across the three core disciplines.

How does your organization measure up?

As we have discussed, balanced maturity across the three IT risk management disciplines can yield major benefits. So how does your organization measure up? To find out, rate your organization on the three groups of statements that follow. They will help you assess your maturity on each core discipline.

To assess your organization's competency in IT risk governance, ask yourself to what extent the following statements describe your organization (1 = not at all, 7 = to a great extent). Then add up your totals.

Rating your IT risk management governance processes

___ We have clearly defined categories—such as availability, access, accuracy and agility—into which IT risks are grouped.

___ We have guidelines to help individuals assess the magnitude of risks in a consistent way.

___ We have a formal process for evaluating potential exceptions to IT policy.

___ We have key indicators to monitor the effectiveness of our IT risk management activities on a regular basis.

___ IT risk management is integrated into risk management for all other enterprise-level risks.

___ Total (out of 35)

Rating your IT foundation

To assess your organization's IT foundation, ask yourself to what extent the following statements describe your organization (1 = not at all, 7 = to a great extent). Then add up your totals.

___ A business continuity plan exists to help my organization recover in the event of an IT infrastructure failure.

___ Our IT environment—including applications, middleware, servers, storage and networks—is well maintained.

___ Our infrastructure and applications environment is no more complex than necessary for the business to run effectively.

___ IT people understand how IT and infrastructure link to business processes.

___ Applications and infrastructure follow a well-defined enterprise architecture.

___ Total (out of 35)

Rating your risk-aware culture

To assess your organization's competence in developing and maintaining a risk-aware culture, ask yourself to what extent the following statements describe your organization (1 = not at all, 7 = to a great extent). Then add up your totals.

___ Employees can talk openly about IT risk.

___ Employees are trained in risks and controls relevant to their roles and responsibilities.

___ There are frequent reminders of IT risks and policies through a variety of communications approaches.

___ Most discussions between IT and business include IT risk implications.

___ Executives commend risk-aware behavior and criticize behavior that is the opposite.

___ Total (out of 35)

Now that you have your scores, you can compare them with those of a typical organization in the figure on the next page. If your organization is lacking in one area, it may be the weak link that makes your business vulnerable to IT risk. When all three areas are at a basic level of maturity, you should continually work to increase maturity in a balanced way to increase your overall IT strength or resilience.

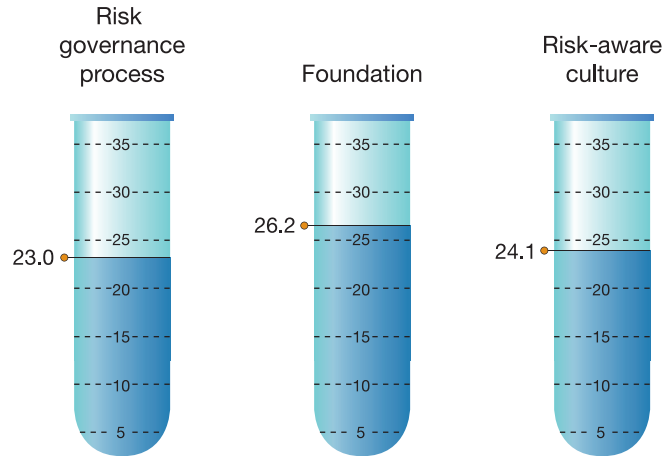


Figure 4

The 258 organizations in our survey reported an average of 23.0 on risk governance process, 26.2 on IT foundation and 24.1 on risk-aware culture. How does your organization compare?

Conclusion

The CIO is in a strong position to use risk management to improve overall business process management. Because senior executives pay close attention to the risk governance process, CIOs can use it to improve risk awareness and make the case for improving the IT foundation. By using the right language—the four A's—to talk about risk and by building balanced maturity to address it, organizations can derive value that goes beyond risk avoidance.

By including risk management in conversations among CIOs, CFOs, LOB leaders and chief risk officers, CIOs can not only reduce incidents but also increase IT efficiency and business agility.





For more information

For more information about tools and support that can help advance the CIO profession, please visit the Center for CIO Leadership:

www.cioleadershipcenter.com

© Copyright IBM Corporation 2009

IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.

Produced in the United States of America
January 2009
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

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

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

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

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

¹ George Westerman and Richard Hunter, *IT Risk: Turning Business Threats into Competitive Advantage*, (Harvard Business School Press, 2007).

² IT Governance Institute, *IT Governance Global Status Report—2008*, March 3, 2008. © 2008 IT Governance Institute. All rights reserved. Used by permission.

³ George Westerman and Richard Hunter, *IT Risk: Turning Business Threats into Competitive Advantage*, (Harvard Business School Press, 2007), 57.

