Driving New Value From IT Risk Management

The economic downturn has created a dual problem for IT organizations. IT risk management is more important than ever, yet spending cuts mean that IT risk management investments must compete for limited funds with initiatives that appear more interesting to business executives. As organizations struggle to squeeze the most value from all monies invested, they find themselves asking how to get more value from their risk management activities. This goes beyond cutting risk management costs and includes using risk management insights to improve the way IT and business processes are managed.

Unfortunately, improving the value of IT risk management is far from straightforward. IT risk management has many faces, with managers in different silos (such as security, business continuity, project management and regulatory compliance) often operating independently. For too long, IT risk management has been caught in a tenuous middle ground between enterprise risk and specialized silos of IT risk efforts. Technology risk managers have had to adapt general risk management guidance to the specialized domain of IT or try to generalize and integrate domain-specific guidance. Both approaches provide some help, but neither can generate the holistic view of IT risk as business risk that is becoming more important in an increasingly digitized and interconnected world. While ISACA’s new Risk IT: Based on CoIT framework is crossing silos of risk management, it can also be seen as creating a larger menu of possible actions from which to select. This leaves professionals asking, “Where should we focus to improve the effectiveness and value of IT risk management?”

This article describes the three disciplines of IT risk management, their implications for risk management value and their context in ISACA frameworks. Companies that achieve maturity on the disciplines not only manage risk better, but also can use IT risk management to improve IT management and business outcomes. Their risk management investments pay new value in four ways: fewer incidents, more efficient IT processes, better alignment with the business and higher agility.

THREE DISCIPLINES OF IT RISK MANAGEMENT

In many organizations, the goal of IT risk management is to ensure that the company does not experience any bad incidents because of IT, whether from unplanned downtime, hacker attack, project overruns or a compliance problem. Organizations have already taken many basic actions in different areas of IT risk management. However, the focus is often on protection, not improvement, on spending, not value. In addition, they often fail to examine how their risk protection activities may decrease agility.

A recent Massachusetts Institute of Technology (MIT) research study found that three IT risk management disciplines work together to address risks to four key enterprise objectives: availability, access, accuracy and agility. Companies that get higher value from IT risk management investments are mature in all three disciplines:

- **An IT foundation** that is well managed and only as complex as necessary
- **A risk governance process** to understand what risks the enterprise faces and to decide what to do about them
- **A risk-aware culture** where people have appropriate awareness of risks and are comfortable talking about them

These three disciplines work together to ensure that an organization understands the IT risks it faces, makes good decisions about them and starts to reduce risk over time.

In mid-2008, the authors of this article surveyed 258 senior executives (100 IT, 158 non-IT) in six countries. Respondents represented a balanced set of executives who self-identified as the most senior IT or business executive involved with IT risk. Survey questions were based on well-defined concepts from prior research, including the MIT Center for Information Systems Research (CISR) research.
Survey items were statistically examined and combined to develop key research constructs, and then correlated and controlled to examine relationships between risk management maturity and important outcomes. The analysis found that each of the three disciplines makes its own contribution to improving the value of IT risk management (see Figure 1). Mature risk governance is necessary but not sufficient. It raises attention to risk, increases stakeholder involvement and provides information for decision making. However, actual improvement comes from driving change in the IT foundation and risk-aware culture. Firms with a more mature culture or foundation report statistically fewer incidents than other firms, but the benefits go farther. They also report statistically significantly higher efficiency, IT-business alignment and agility.

Figure 1—How the Three Risk Disciplines Relate to Business Performance

The IT risk management survey of 258 IT and non-IT executives finds firms that are more mature in the foundation and risk-aware culture (not just the risk governance process) also have higher business performance, not just fewer incidents.

Although protecting the foundation and building awareness are familiar elements to ConT™ users, IT risk managers should go beyond these protections.

The goal of the risk governance process should be to improve the foundation and create a risk-aware culture, not just protect a shaky foundation or conduct awareness training. To cite a non-IT example, risk governance has been credited with reducing deaths in commercial aviation. That benefit was delivered not directly through the risk governance process, but through better design and maintenance of airplanes, plus creation of a risk-conscious culture among crew members. In IT terms, ConT provides guidance on planning, implementing delivering and monitoring investments in, and operations of, an organization’s IT foundation, including investments that reduce risk. In many IT situations, enterprises add protection and sometimes help to prevent maintenance issues. This is not enough. Enterprises frequently get only limited value from risk management because they invest only in protecting a poorly designed foundation instead of working to make the foundation less complex. Back to the airline example, more gauges in an airplane cockpit give pilots a better view of performance and problems, but they do not fix design problems in the engines.

What Does It Mean to Be More Mature in the Three Disciplines?

The risk governance process is the set of policies, processes and roles that enables an organization to exercise oversight and make better decisions about IT risks. In most firms, a central group creates policies and processes for the enterprise. Local managers identify and address the risks while notifying the central group about the highest risks. An enterprise-wide committee prioritizes how to invest in mitigating the firm’s highest risks, while local managers address lower risks on their own. Firms that are more mature in risk governance have clear risk categories, guidelines to assess risk consistently, formal exception processes and key risk indicators. They have also taken action to integrate their IT and enterprise risk processes.

No process improves without a process owner, but only half (48 percent) of firms have placed a single person in charge of IT risk management, according to the authors’ survey. Only about a third of companies have either formal categories of risk or a formal exception process. Formal categories help to identify and compare risks in an apples-to-apples way. The exception process is even more important, since exceptions are how organizations learn. Exceptions also increase operations risk in the IT foundation by increasing complexity, meaning they should get special attention both during projects and afterward.

Only 28 percent of respondents to the survey say they use key risk indicators (KRIs) effectively. A fully integrated KRI dashboard is difficult to achieve, but firms can start with simpler measures. Financial services firm PFPC (now PNC Global Investment Servicing) started by tracking trouble-ticket volume and employee turnover. Other firms track...
indicators such as password resets, project completion rates, reconciliation failures, recovery times and intrusion attempts. In the current environment, it is essential to become more sophisticated in gathering, trending and acting upon KRI's, as well as in linking these to control design.

An important issue is the 66 percent of firms that have not effectively integrated IT risk into enterprise risk management (ERM). General-purpose ERM frameworks such as A Risk Management Standard (ARMS), AS/NZS 43609 or the COSO ERM framework do not explicitly address IT risk, but Risk IT enables companies to map from broader ERM frameworks to business process dependencies on technology.

The IT foundation is the set of infrastructure, applications, supporting technology and IT people who enable business processes to run. Firms with a mature IT foundation have a well-managed infrastructure, a well-defined business continuity plan, and a solid understanding of the links between technology and business process. But, they go beyond this. They also have enterprise architecture in place and are working to ensure that the IT foundation is no more complex than necessary.

An immature IT foundation—overly complex or poorly managed—is a recipe for risk. Inconsistent software updates and overly complex interdependencies cause it to fail often, make it difficult to recover, and make it more difficult to change. An immature IT foundation eats up maintenance resources and restricts agility.

While three-fifths of respondents reported that they maintain infrastructure well and have a working business continuity plan, it is important to stay vigilant. One firm experienced the same virus at three offices, six months apart, because IT staff in the affected sites did not inform other sites of the vulnerability. At another firm, IT staff routinely missed a set of servers when installing patches. Key to keeping the IT foundation well maintained are well-designed and well-maintained controls, such as those in ConT, and operational management processes, such as those in the IT Infrastructure Library (ITIL). In ConT terms, these are the Deliver and Support (DS) and Monitor and Evaluate (ME) processes.

Although the majority of firms are satisfied with their infrastructure maintenance, not as many are taking the important step of reducing complexity in their IT foundation. Only about 40 percent believe their IT foundations are no more complex than necessary, or that their people understand the links between IT and business processes. Risk Evaluation (RE) processes in Risk IT can be helpful here, especially RE.3.1 (Map IT resources to business processes) and those immediately following. Managers can use a risk-return approach to justify some investments that might not have a clear return-only business case. They can also use risk evaluation activities to identify ways to improve business processes, not just protect or control them. Then, they can use project-level IT governance mechanisms (such ConT's Acquire and Implement [AI] processes and Val IT's Investment Management [IM] processes) to gradually reduce complexity in the foundation over time.

For example, in prioritizing and conducting projects, several firms have begun to include architectural standards and complexity issues in their decisions. Intel prioritizes projects not only based on strategic alignment and expected financial return, but also on alignment with the firm's architectural direction. A consumer food manufacturer introduced risk-focused checkpoints into its project demand management and delivery processes.

The risk-aware culture is the third discipline. This is not a risk-averse culture, and it is not a company that just does awareness training. It is a culture where people recognize the risks inherent in their activities, can openly discuss their risks, and are willing to work together to resolve risks or incidents. Having a mature risk-aware culture makes a firm both safer and more agile. People know how to avoid overly risky behaviors and resolve conditions that introduce unnecessary risk. However, they constantly balance this ability with the recognition that too much protection can introduce agility risks (i.e., rigidity). When people understand which risks are worth taking and understand which conditions and behaviors introduce unwanted risk, the firm can take on more risk in pursuit of return.

A mature risk-aware culture does not happen accidentally. It must be consciously built and reinforced by the company's leaders. Companies with a mature risk-aware culture have employees who understand risk and controls relevant to their jobs, who can talk openly about risk without fear of reprisal, who include risk in their business conversations, and who are encouraged through frequent reminders and top leadership reinforcement.
Three-fifths of respondents said their employees are comfortable talking openly about IT risks, but only about a third had effective risk training or reinforced it with reminders. Still fewer used risk awareness to improve the way they make IT decisions, as only 27 percent said most IT-business discussions include risk. Discussing IT risk issues, such as how tightly to integrate an acquired unit’s IT assets or whether to use a nonstandard set of technologies in a project, can be a useful way to identify approaches that achieve the intended business benefit while also reducing operational risks. Furthermore, making clear the risk implications of a new mobile device, rather than just saying “it is too risky,” can go a long way to not only making better decisions, but also to improving risk awareness and alignment.

The goal is to make the risk-aware culture in IT as prevalent as the safety culture in high-risk industries. Nearly every big oil company requires that meetings start with a short discussion on a safety topic. There are frequent safety reminders. Executives in these firms make a point of discussing risk and noting when people are being risk-unaware. IT leaders can use similar practices to make their units’ cultures more risk-aware. This discipline corresponds to the risk culture discussion in section 3 of ISACA’s The Risk IT Practitioner Guide and to Risk IT’s Risk Governance (RG) processes 1 and 2 (especially RG1.5).

Driving New Value Through Risk Management Maturity

Most enterprises have made some progress on each of the disciplines, but maturity varies. To an ISACA member and CobiT user, the importance of controlling the IT foundation is clear. However, CobiT places less emphasis on reducing complexity in the foundation, building a risk-aware culture and increasing risk governance maturity. Risk IT extends CobiT with significant emphasis on risk governance and culture, but neither CobiT nor Risk IT specializes in architectural simplification. The survey findings suggest actions IT risk managers can use to drive more business value from IT risk management activities—improving IT management, not just protecting against IT incidents.

First, balanced maturity matters. Maturity in one or two of the three disciplines was not as strongly associated with positive outcomes as maturity across all three. For example, focusing on CobiT DS processes without sufficient investment in, say, Risk IT RE processes creates the potential for misdirected or even wasted spending on various fixes. Similarly, building great risk governance without going on to improve the IT foundation and risk-aware culture is like being all dressed up with nowhere to go. Especially in this tough economy, risk managers must focus on creative and thoughtful approaches to investment and value, not just fixing the most visible risks.

Second, maturity must be assessed and improved across the disciplines. Risk managers can assess their organizations against maturity models in Risk IT or other frameworks. Then, they should identify gaps in each discipline and work to bring all up to appropriate maturity. For example, if an enterprise is a strong CobiT shop, it likely has several mechanisms to improve areas such as networks or storage, but may struggle to build business cases around them. In this situation, it is probably wise to increase maturity in risk governance to improve alignment and gain stakeholder support for their investments. The governance process may be more mature in companies that focus on compliance or audit, but risk managers may struggle to “get beyond reporting” and show real business impact. Still others may be protecting an overly complex foundation without identifying opportunities to reduce operations risk by reducing complexity.

Third, IT risk management concepts must be integrated more tightly into other IT and business management processes. Managers who link IT risk to business objectives and outcomes can make the case for moving the IT foundation in the right direction—getting less complex, not just better managed. They also increase the risk-aware culture by helping everyone understand what drives operational IT risks and by making the risk implications of key IT decisions more apparent. By creating risk-based cost scenarios, they can help IT and business executives better align their expectations.

Also, by influencing decisions rather than trying to protect the results of risk-blind decisions, risk governance can pay off twice. It reduces negative incidents and increases business benefit by maturing the foundation. For example, operational risk managers at a major credit card company and at a Canadian bank both reported that, when examining risks in their business processes, they discovered useful ways to reengineer the processes. Their initial investments in risk management largely paid for themselves through improved business efficiency and service quality.

Finally, to improve outcomes from their activities, IT risk leaders can join forces with others who have shared objectives. Managers in IT governance, enterprise architecture, business continuity, compliance, security and project portfolio management all have reasons to emphasize risk as well as return, less complexity over more, and a more
Companies that are mature in all three disciplines—risk governance process, IT foundation and risk-aware culture—have statistically significantly fewer incidents, higher IT efficiency, better alignment and higher business agility. But maturity means more than just doing the basics. It is more than identifying risks, protecting existing assets and increasing awareness of threats. Companies with mature risk management capability use risk governance to reduce complexity in the foundation. They go beyond awareness to build a culture in which safe discussion of risk (from availability through agility) is the norm. These companies not only prevent risk, but also can take new risks safely. They not only reduce incidents, but also improve efficiency. Then, the company’s investments in risk management pay off not only in better risk management, but also in better IT management and business results.

AUTHORS’ NOTE

The authors continue their research into IT and enterprise risk management. If you are interested in being a case study or survey participant, please contact George Westerman at georgew@mit.edu or Brian Barnier at brian@valuebridgeadvisors.com.

ENDNOTES


3 Op cit, Westerman and Hunter

4 ConIT (IT Governance Institute, 1996-2007) is an IT governance framework and supporting tool set that allows managers to bridge the gaps among control requirements, technical issues and business risks. ConIT enables clear policy development and good practice for IT control throughout organizations. More information is available at www.isaca.org/cobit.

5 As defined in Risk IT (ISACA, 2009, www.isaca.org/riskit), “Any metric showing that the enterprise is subject to, or has a high probability of being subject to, a risk that exceeds the defined risk tolerance is a KRI.” KRIs are described in more detail in section 7, “Essentials of Risk Response,” of Risk IT.


7 Op cit, Westerman and Hunter


10 Committee of Sponsoring Organizations (COSO) of the Treadway Commission, Enterprise Risk Management—Integrated Framework (COSO ERM), 2004. This should not be confused with the COSO Control Framework that is familiar to many ConIT practitioners. A summary of COSO ERM is available at www.coso.org.


12 Val IT (ISACA, 2008, www.isaca.org/valit) is an ISACA framework and supporting publications addressing the governance of IT-enabled business investments.

13 To cover this, ISACA provides a 281-page mapping from ConIT to The Open Group Architecture Framework (TOGAF). See ISACA, ConIT® Mapping: Mapping of TOGAF 8.1 With ConIT® 4.0, 2007, www.isaca.org/cobitmapping.

14 Readers are welcome to contact the authors for the short set of assessment questions used in their research.