CENTER FOR
INFORMATION
SYSTEMS
RESEARCH

Sloan School
of Management

Massachusetts
Institute of
Technology

Cambridge
Massachusetts

# IT Risk Management: From IT Necessity to Strategic Business Value

George Westerman

*December 2006*

**CISR WP No. 366 and MIT Sloan WP No. 4658-07**

- □ **Research Article:** a completed research article drawing on one or more CISR research projects that presents management frameworks, findings and recommendations.
- □ **Research Summary:** a summary of a research project with preliminary findings.
- ☑ **Research Briefings:** a collection of short executive summaries of key findings from research projects.
- □ **Case Study:** an in-depth description of a firm's approach to an IT management issue (intended for MBA and executive education).
- □ **Technical Research Report:** a traditional academically rigorous research paper with detailed methodology, analysis, findings and references.

**CISR Working Paper No. 366**

**Title:** **IT Risk Management: From IT Necessity to Strategic Business Value**

**Author:** **George Westerman**

**Date:** **December 2006**

**Abstract:** With information technology becoming an increasingly important part of every enterprise, managing IT risk has become critically important for CIOs and their business counterparts. However, the complexity of IT makes it very difficult to understand and make good decisions about IT risks. CISR research has identified four business risks — Availability, Access, Accuracy, and Agility — that are most affected by IT. Since nearly every major IT decision involves conscious or unconscious tradeoffs among the four IT risks, IT and business executives must understand and prioritize their enterprise's position on each. Three core disciplines — IT foundation, risk governance process, and risk aware culture — constitute an effective risk management capability. Enterprises that build the three core disciplines manage risk more effectively and their business executives have better understanding of their IT risk profile and risk tradeoffs. When done well, IT risk management matures from a set of difficult compliance and threat-reduction activities to become a true source of agility and business value.

Keywords: IT related risk, IT governance, IT architecture, business agility.

*12 Pages*

Center for Information Systems Research
Sloan School of Management
Massachusetts Institute of Technology
RESEARCH BRIEFING
MITSloan

Volume IV Number 1C March, 2004

# Understanding the Enterprise's IT Risk Profile[1]

**George Westerman,** *Research Scientist*
*MIT Sloan Center for Information Systems Research*

Every enterprise faces a large number of risks as part of doing business. Some risks, such as the loss of a key executive, are not IT related. Others, such as global credit risk, have an important IT component, but are largely business-driven. There are four dimensions along which IT itself constitutes a risk to the enterprise (see Figure 1). These risks arise from the way the enterprise's existing IT assets and processes are arranged, as a result of managerial tradeoffs made over many years. Understanding the firm's levels of risk and risk tolerance along these four dimensions is the first step in implementing a mature IT risk management process. In this research briefing, the four dimensions and their drivers are described. Case examples illustrate the nature of these risks and the tradeoffs inherent in managing them.

## *Research Method*

To develop the Enterprise IT risk framework, we interviewed 45 senior IT and business managers in 12 firms. We asked them to talk about the types of enterprise risk influenced by their IT assets, organizations, and processes. We also asked what conditions increase risk, and what practices reduce it. After consolidating more than 700 items from the interviews, we identified a list of more than 100 risk factors, in six categories, that influenced a risk dimension.

## *Defining the Four Dimensions*

A working definition of "risk" is a potential exposure that can impact an important organizational objective. An enterprise IT risk is a potential exposure facing the enterprise as a result of any aspect of the IT environment. This includes IT assets, organization or processes.

The four dimensions of Enterprise IT Risk correspond to four enterprise-level objectives of IT:

- *Availability*: keeping existing processes running, and recovering from interruptions.
- *Access*: ensuring that people have appropriate access to information and facilities they need, but that unauthorized people do not gain access.
- *Accuracy*: providing accurate, timely and complete information that meets requirements of management, staff, customers, suppliers and regulators.
- *Agility*: implementing new strategic initiatives, such as acquiring a firm, completing a major business process redesign or launching a new product/service.

Each initiative for IT funding, organization, sourcing and technology shapes an organization's risk profile for the short and long term. The initiative can affect the likelihood of an adverse event, its impact (financial, reputational or otherwise), or both.

For example, some firms are implementing "single sign-on" capability, in which people can use a single user ID to access many applications. The move, which is aimed at improving user satisfaction, is also seen as improving risk management. Unfortunately, in many implementations, this is only partly true. Single sign-on can reduce the *likelihood* of an intrusion, since security personnel can focus on a single access point, and users are more likely to follow security policy if they have only a single user ID. But, many single-sign-on implementations actually increase the *impact* of an intrusion, since a single intruder has access to more data.

This example illustrates how IT risk management is much more complex than just implementing technology. There are other categories of risk factors (see the bottom of Figure 1). The enterprise must compartmentalize information, understanding which users should have access to what applications and information. Policies must be created in keeping with the security/privacy needs of the organization as well as its customers and regulators. IT must

[1] This research was made possible by CISR sponsors and, in particular, CISR Patrons Gartner and DiamondCluster International. The author also wishes to thank research associates Michelle Salazar, Zheng (Philip) Sun, and Robert Walpole.

have staff who can responsively administer user access, and must train all users and vendors in the procedures. By considering each of the six categories of risk factors, managers can avoid missing an important piece of the puzzle.

### *The Enterprise Risk Profile*

Few organizations, when considering a new initiative, go beyond ROI to consider the effect on the enterprise risk profile. The single sign-on example was within a single risk dimension, but most IT arrangements affect multiple dimensions. Unfortunately, many decisions are made without considering all four risk dimensions. Many firms fall into patterns where one type of risk (most commonly availability) is prioritized over others. Or, worse, they routinely fail to examine one or more dimensions of risk. Over time, a series of incremental decisions, each one following the firm's standard practice, leads to a risk profile in which some risks are well controlled while others have huge (and often unknown) exposures.

Figure 2 shows the Risk Profile: a tool to communicate the enterprise's relative risk exposure and tolerance on the four dimensions. The blue diamond represents the potential level of risk to the business as a whole, before any risk management is undertaken. The maroon represents the IT component of enterprise risk, along each category. The green inner diamond represents IT risk tolerance, meaning the amount of IT risk that the enterprise chooses to live with. Finally, the beige represents the risk gap—the amount of risk that has not yet been mitigated.[2]

The risk profile in Figure 2 is for GCI, a large global manufacturing firm.[3] To compete in very tough markets, GCI relies on strategic agility enabled by frequently buying and selling firms. To address agility risk, GCI moves each acquired firm to a standard technical infrastructure, but keeps the applications intact and under the control of the business unit manager. By standardizing infrastructure, the firm reduces costs and somewhat reduces availability risks. By keeping each business unit's unique applications under the control of the business unit manager, GCI believes it reduces agility and availability risks.

Unfortunately, GCI's approach has led, over time, to a large gap on access risk (see point A on Figure 2). Dozens of global or local applications each have their own passwords and security procedures. Copies of competition-sensitive information, such as the global business plan, are stored locally in each site.

In addition, there is a large gap on accuracy risk (see point B). To get a global snapshot of financials, the CFO asks managers in each business unit to manually upload data into a data warehouse. The manual process was much less expensive than a proposed $10Million automated solution, and it works well. But financial data is up-to-date only twice per month, and financial processes cannot be fully certified for Sarbanes-Oxley.

GCI's IT managers are currently identifying initiatives to address the risk gaps in access and accuracy. In keeping with GCI's decentralized philosophy, these initiatives will not require standardizing all systems globally. Instead, they will involve automatically integrating information from disparate applications, and coordinating, rather than centrally controlling, user access. In addition, senior executives may choose to 'live with' the manual financial process, but add manual controls to ensure financial data integrity.

### *Using the Risk Profile and Risk Framework*

The risk profile (Figure 2) can be created for the enterprise as a whole, or for important parts such as major business units, major global regions or even critical business processes. The profile can be linked to the funding process, so that initiatives that reduce risk gaps receive priority over those that do little to reduce risk. Then, managers can use the risk framework (Figure 1) to ensure that each initiative addresses all categories of risk factors.

The risk profile can also be a negotiating tool. Many disagreements over IT priorities can be traced to differing risk perceptions. Comparing each manager's perception of enterprise risk exposure (beige diamond) and risk tolerance (green diamond) can resolve disputes and help forge a common direction for the future.

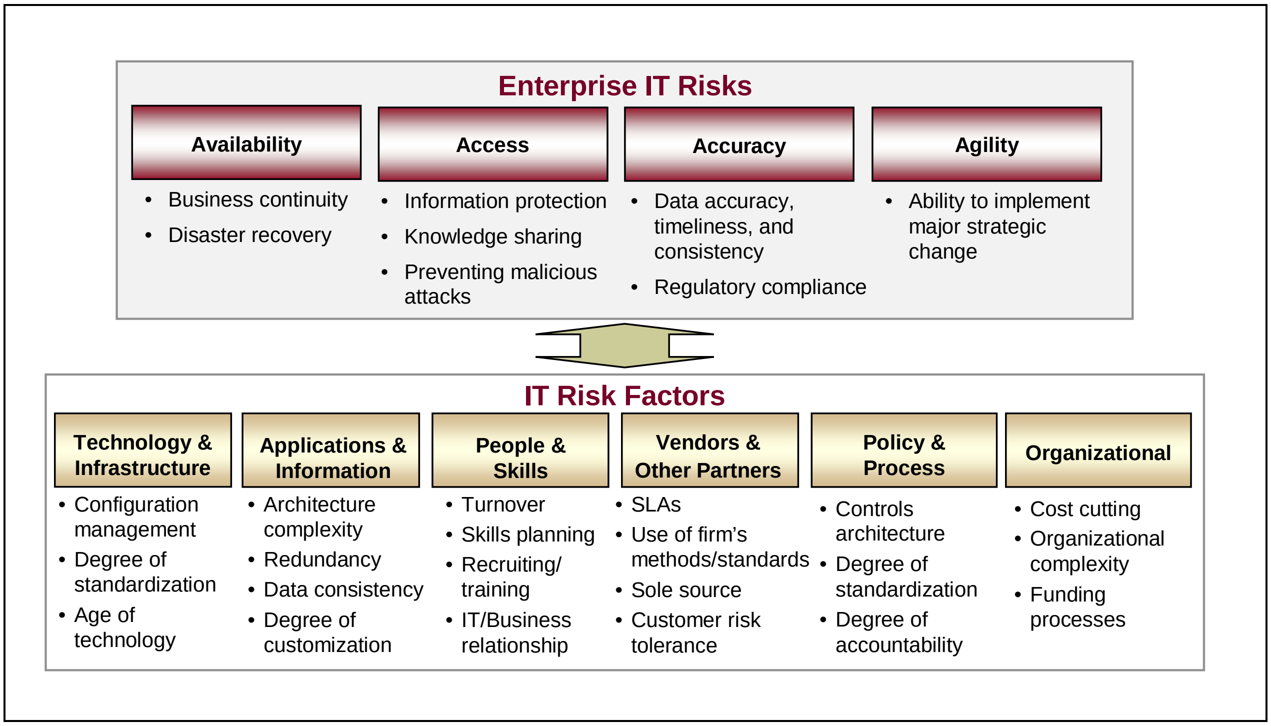
In combination with a mature risk management process (which will be discussed in a future research briefing), the risk framework and risk profile tools

[2] The profile can be generated using either top-down or bottom-up methods. Many managers find that, by trying to plot risks and risk tolerances subjectively on a 0 to 10 scale for each dimension, they come to a better understanding of the tradeoffs and risk tolerances facing the enterprise. Others use the tool in a bottom-up way, consolidating very detailed information from their risk tracking databases into a single picture. Either way, the risk profile is a valuable way to communicate enterprise IT risks to senior executives. We have developed of questionnaire to assess a firm's IT risk and generate their risk profile.

[3] This is a disguised name for a large, well-known manufacturer.

can improve risk awareness and reduce IT-related exposures. Awareness of risks enables managers to efficiently prioritize which risks they'll reduce and, just as importantly, to choose which risks they'll accept.

**Figure 1: Enterprise IT Risk Framework**



Enterprise IT Risks

**Availability**
- Business continuity
- Disaster recovery

**Access**
- Information protection
- Knowledge sharing
- Preventing malicious attacks

**Accuracy**
- Data accuracy, timeliness, and consistency
- Regulatory compliance

**Agility**
- Ability to implement major strategic change

IT Risk Factors

**Technology & Infrastructure**
- Configuration management
- Degree of standardization
- Age of technology

**Applications & Information**
- Architecture complexity
- Redundancy
- Data consistency
- Degree of customization

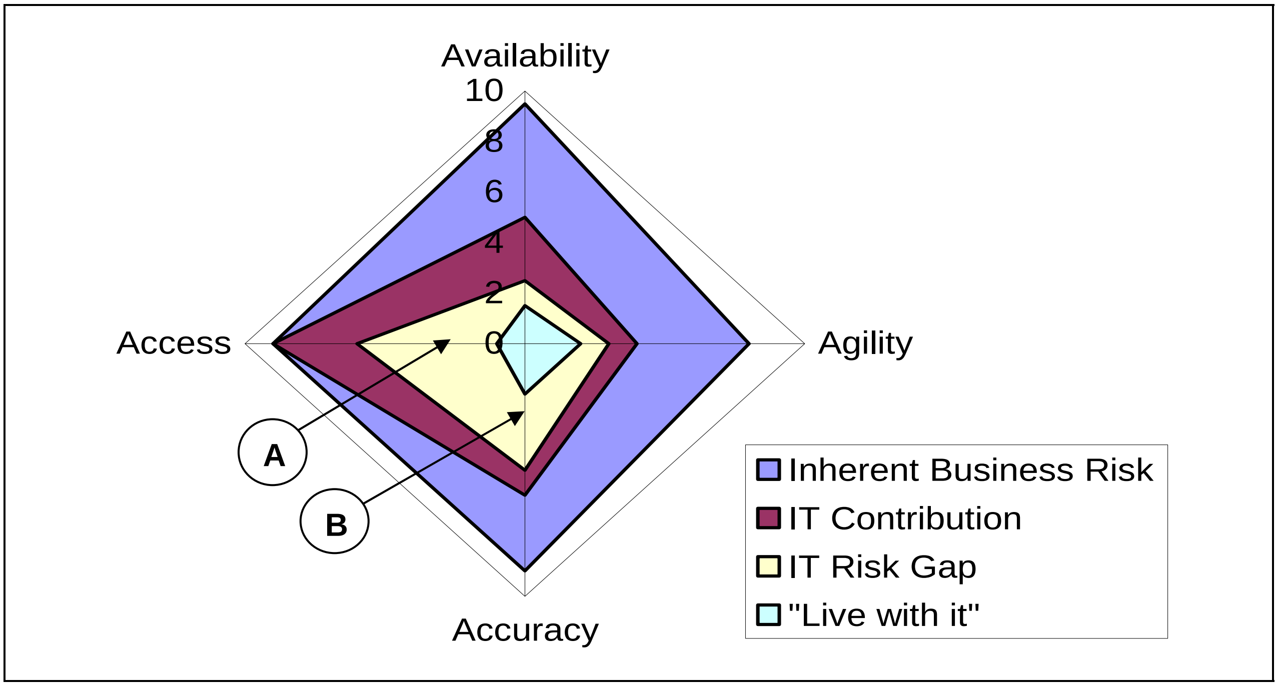
**People & Skills**
- Turnover
- Skills planning
- Recruiting/ training
- IT/Business relationship

**Vendors & Other Partners**
- SLAs
- Use of firm's methods/standards
- Sole source
- Customer risk tolerance

**Policy & Process**
- Controls architecture
- Degree of standardization
- Degree of accountability

**Organizational**
- Cost cutting
- Organizational complexity
- Funding processes

**Figure 2: Risk Profile for Global Components, Inc.**



Center for Information Systems Research
Sloan School of Management
Massachusetts Institute of Technology
RESEARCH BRIEFING
MITSloan

Volume IV Number 2C July 2004

# Building IT Risk Management Effectiveness

**George Westerman**, Research Scientist
MIT Sloan Center for Information Systems Research

## *Introduction*

IT Risk Management is gaining visibility in the world's enterprises. Enterprises are considering not only technical risks, but also how IT risks influence enterprise-level risks. The executive's view of IT risk is moving beyond availability and access management to examine implications of information accuracy and strategic agility.

Effective risk management capability has a number of payoffs. Enterprises that manage risk effectively have a better handle on how they are addressing high priority risks and importantly, what risks they are choosing to "live with." They are confident that they are focusing money and effort on risks that really matter. And, they can go after opportunities that other enterprises would find too risky to undertake.

Unfortunately, few enterprises are mature in their ability to manage enterprise IT risks. Most enterprises use an intuitive approach to risk management: they address high-profile risks that get media attention (such as viruses or power outages or wireless), but subsequently miss many risks that are lower-profile (such as inadequate internal controls or aging, brittle applications).

## *Building Effective Risk Management*

How can an enterprise build risk management capability? In interviews with more than 50 IT managers, we found that effective risk management is a cohesive combination of three core disciplines (see Figure 1):

- Risk governance process: complete and effective risk-related policies, combined with a mature, consistent process to identify, assess, prioritize, and monitor risks over time.
- Risk aware culture: skilled people who know how to identify and assess threats and implement effective risk mitigation.
- Effective IT foundation: IT infrastructure and applications that have inherently lower risk because they are well-architected and well-managed.

If a firm is severely lacking on any of the three disciplines, it cannot be effective at IT risk management. For example, no level of governance process or expertise can overcome a complex, overly-risky foundation. Similarly, heavy risk governance cannot be effective without the expertise to identify and reduce risks.

However, firms need not be world class in all three disciplines; rather, they can be world-class in one, with lower (but still acceptable) levels in the other two. Moreover, firms that have ineffective risk management cannot become effective overnight; they build capability over time by using one discipline very well to help the others grow to an effective level.

The remainder of this briefing describes the approaches taken by three global companies to build effective IT risk management. Each used a different discipline as the driver of its risk management efforts.

## *1. FinCo: Leading with Risk Governance*

FinCo, a provider of services to financial services firms, was highly dependent on IT. Unfortunately, auditors were increasingly expressing concern about the state of FinCo's IT risk profile. Having grown very rapidly, FinCo had numerous application silos on a variety of platforms. Each of eleven business units had its own IT staff, with varying views of risk management. There was little internal expertise for IT risk management.

Risk management was one of the newly-appointed enterprise CIO's first initiatives. Since changing the installed base would require extensive time and effort, and since it would be difficult to build a large group of risk experts quickly, FinCo focused on implementing strong risk governance process. They established policies and plans for business continuity, access management, information retention, system development methodology, vendor management and other areas. They conducted risk identification exercises to identify and prioritize risks. They established a tracking process to show whether risks were being mitigated as planned. Finally, they implemented risk-related reviews throughout the project initiation process, so that new projects either complied with risk policy or were immediately noted as exceptions.

The result was a lopsided risk management "propeller" (Figure 2a), driven by the heavy blade of risk governance process. Over time, this is evolving to a more stable cohesive arrangement (Figure 2b). By participating in risk governance processes, IT employees have increased their risk awareness and senior management has begun to understand the importance of IT risk management. Meanwhile, the process identifies high-value risk reduction opportunities for the foundation, and ongoing project reviews ensure that the foundation doesn't get more risky over time.

Effective IT risk management has paid dividends by showing auditors how serious FinCo is about risk management, and by increasing the firm's credibility with potential corporate clients. It has also built business (and client) buy-in as FinCo revamps its entire applications architecture.

## 2. EquipCo: Leading with Awareness

EquipCo, a global supplier of telecommunications equipment and services, took a different approach to building IT risk management effectiveness. Its IT foundation was very complex due to the firm's diverse business units and global scope. Heavy centralized risk governance was not seen as an option because business units had strong IT groups and faced differing environments. However, EquipCo had a great deal of security expertise, since security was an important component of the value proposition for its products and services.

EquipCo decided to lead risk management through awareness, led by a core team of experts. It augmented internal security experts by recruiting experienced risk experts. The 30-person core risk group conducted risk assessments and provided risk mitigation expertise to the business unit IT groups. They also worked with each business unit IT director to prioritize risks and justify risk-related funding.

Instead of heavy enterprise-level risk management processes, the team established corporate policies (for example, in supplier connectivity) that business units can implement through customized local procedures. In addition, the corporate IT risk group actively communicates with business units to help them grow their own risk expertise. The initial risk exercises let by the core team, plus frequent advice and communication, has increased awareness in each business unit. Over time, the combination of strong awareness and lighter risk governance is improving the risk profile of the foundation.

## 3. ChipCo: Leading with Foundation

ChipCo's CIO has, during ten years in his position, taken a different approach to building risk management capability. He and his staff have created an IT foundation that is inherently less risky than other firms. A global semiconductor manufacturer, ChipCo has a single global instance of ERP, linked to standardized manufacturing systems in each fabrication site, all riding on a secure, redundant, standardized infrastructure for processing and networking.

By building a world-class IT installed base, ChipCo is able to use much lighter awareness and risk governance activities but still manage risk effectively. For example, there is no formal core of IT risk staff. IT staff members throughout the firm actively identify and prioritize emerging threats to the foundation, using trade press and their links with other firms.

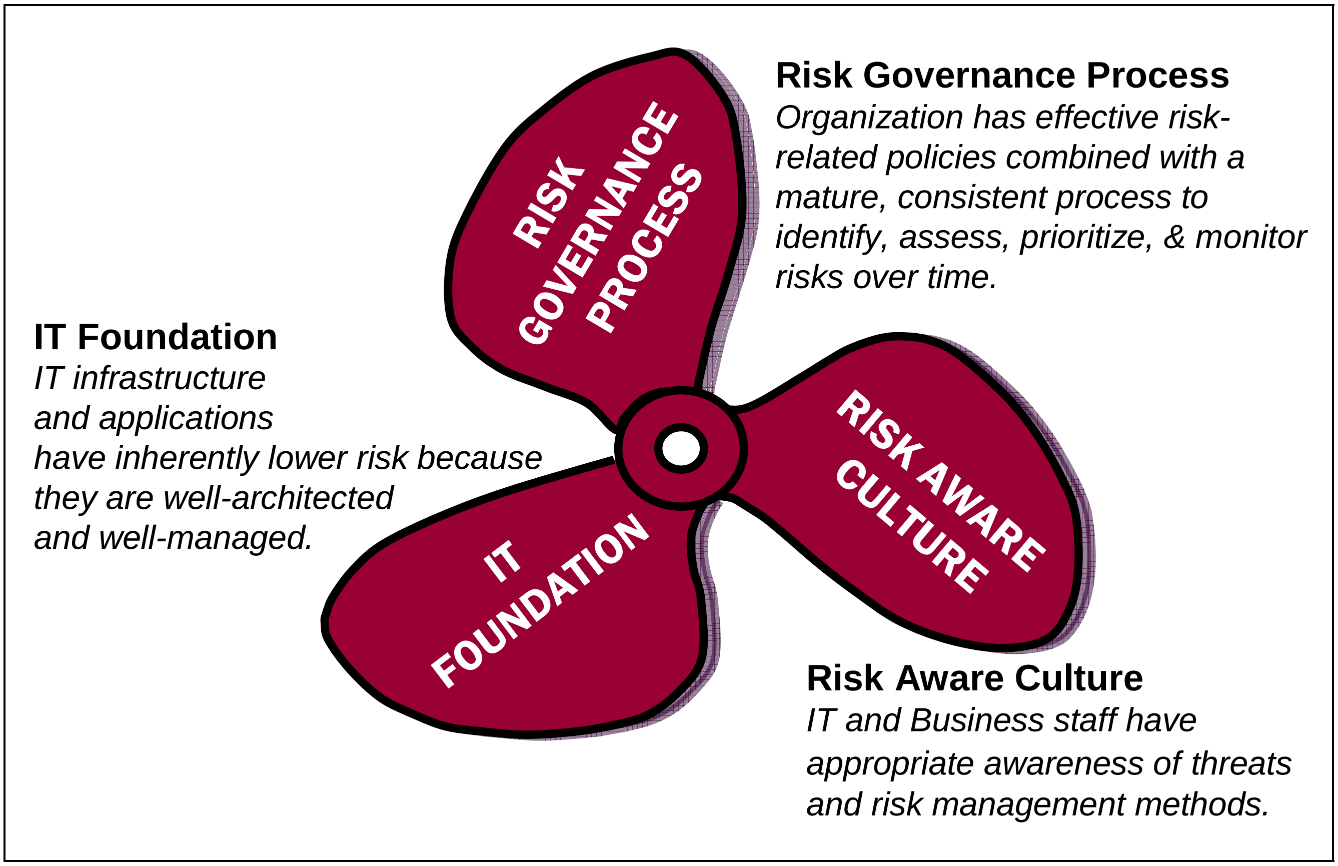
Risk governance is focused on policy and monitoring, but not on formal risk management processes. ChipCo actively monitors its infrastructure and applications for availability and access issues. It has policies in place, such as a freeze on production software changes during a two-week window around quarterly financial close, to reduce the likelihood of an incident. It also has checkpoints in project initiation reviews to identify potential risk issues. The CIO sees no need for a formal, quarterly risk identification and tracking process: *"We take the lead to let the corporation know what we perceive as the biggest threats, and if we need a major capital expenditure or policy change, we bring it to them. But mostly, we're empowered to address the IT risks we see as most important."*

## Conclusion

Effective IT risk management requires three core disciplines. First, a well-architected, well-managed IT foundation is inherently less risky than a more complex one. Second, a mature risk governance process includes policies and procedures to identify and assess risks and prevent risky behavior. Third, risk awareness helps everyone in the enterprise understand threats and mitigation opportunities.

Enterprises need all three disciplines to be effective at risk management, but they need not be world-class at all three. And, they can use one to evolve the others to effective levels. FinCo used regulatory pressure and management commitment to launch a strong formal risk governance process that improved awareness and foundation over time. EquipCo used its security expertise to improve awareness throughout the firm. It could establish risk governance that is less heavy than FinCo's but still effective for improving the foundation. ChipCo, with its very clean foundation, can focus lighter risk governance and awareness on addressing emerging threats. Over time, each of the three firms is evolving a cohesive, stable combination of the three risk disciplines to provide highly effective IT risk management.

Figure 1: Three Core Disciplines of IT Risk Management



**Risk Governance Process**
*Organization has effective risk-related policies combined with a mature, consistent process to identify, assess, prioritize, & monitor risks over time.*

**IT Foundation**
*IT infrastructure and applications have inherently lower risk because they are well-architected and well-managed.*

**Risk Aware Culture**
*IT and Business staff have appropriate awareness of threats and risk management methods.*

Figure 2a: FinCo's Risk Management Capabilities (at launch)

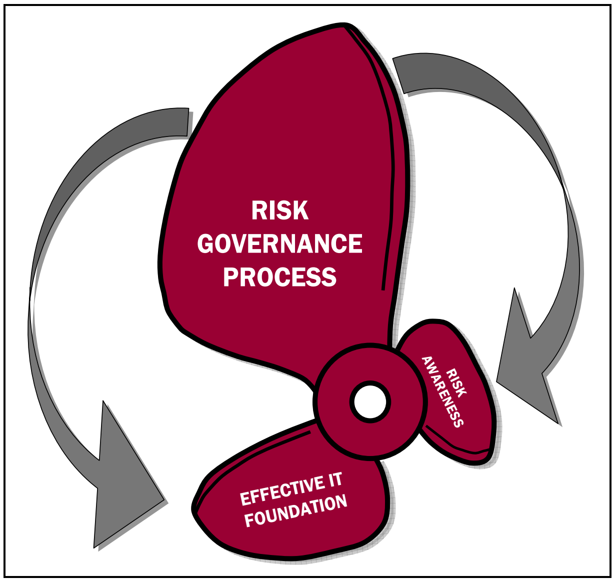
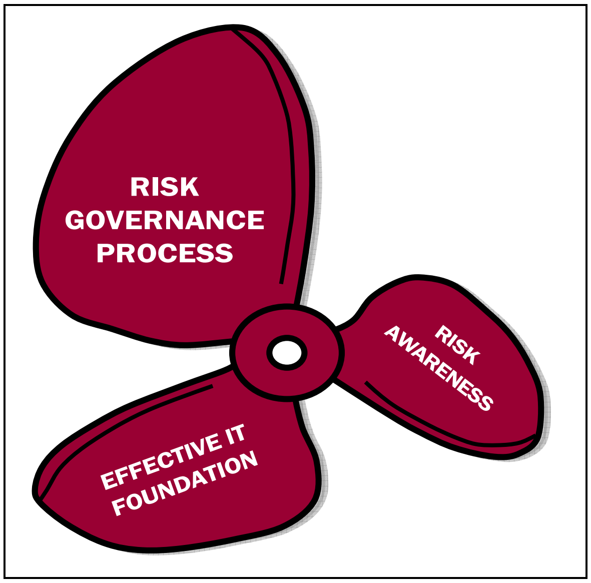


Figure 2b: FinCo's More Balanced Capabilities



Center for Information Systems Research
Sloan School of Management
Massachusetts Institute of Technology

RESEARCH BRIEFING

MITSloan MANAGEMENT

Volume V | Number 1D | March 2005 (Revised April 2006)

# THE IT RISK PYRAMID: WHERE TO START WITH RISK MANAGEMENT

**George Westerman**, *Research Scientist*
*MIT Sloan Center for Information Systems Research*

IT risk management has reached the top of the agenda for CIOs and their senior management colleagues. These executives realize that effective IT oversight requires not only monitoring IT performance, but also understanding the risks that IT creates for the enterprise. Unfortunately, the risk management methods used in most enterprises are unable to cope with the complexity of IT risks, leaving the enterprise vulnerable to costly IT "surprises."

This briefing, based on a survey of more than 130 IT executives, helps resolve the complexity of risk management by identifying key drivers of IT risk and describing a path IT executives can follow to manage IT risk effectively.

Prior CISR research has identified four enterprise-level risks that are most affected by IT assets and processes:[1]

- *Availability*: keeping existing processes running, and recovering from interruptions.
- *Access*: ensuring that authorized people have access to information and facilities they need, and that unauthorized people do not gain access.
- *Accuracy*: providing accurate, timely and complete information that meets the requirements of management, staff, customers, suppliers and regulators.
- *Agility*: implementing new strategic initiatives, such as acquiring a firm, completing a major business process redesign or launching a new product/service.

### *Multiple Factors Drive the Four Risks*

IT risks arise from the way IT applications, infrastructure, people, and policies are organized and managed. Non-standard technologies, inconsistent application maintenance processes, ineffective policies, or missing skills are just some of the factors that create continuity, access management, integrity and strategic change risks. Each risk factor results from a series of conscious or unconscious tradeoffs over time. Assumptions and tradeoffs built into "the way we do things around here" can reduce some risks while increasing others.

For example, a global manufacturing firm had a policy of keeping acquired firms' systems separate from each other, integrating infrastructure only. Senior executives believed this reduced availability risk, since the manager of each factory controlled the resources that ran the factory's IT systems. They also believed it reduced agility risk because leaving systems un-integrated made it easier to buy and sell businesses.

Unfortunately, having more than 20 different ERP versions in-house meant that continuity risk varied across the globe, depending on the skill and conscientiousness of IT technicians in each plant. In addition, the diverse platforms created unacceptable global risks for access and accuracy. Agility risks increased when the large number of applications prevented the firm from implementing global changes required to meet competitive pressures.

### *Risk Factors Are Interdependent*

Figure 1 shows key factors associated with each IT risk, based on statistical analysis of the survey data. Each tier of the pyramid represents one of the four IT risks. Enterprises that are worse on any factor in a risk "tier" report statistically significantly higher levels of that risk. For example, uncompartmentalized data increases access risk because it increases the difficulty of administering user access and also increases the amount of data that can be compromised by an intrusion.

The risk factors form a hierarchy. Factors at the base of the pyramid increase availability risk but also

[1] See *Understanding the Enterprise's IT Risk Profile*, MIT Sloan CISR Research Briefing Vol. IV, No. 1C, March 2004.

increase access, accuracy, and agility risk. Factors in the second tier of the pyramid increase access risk but also increase accuracy and agility risk, and so on.

Non-standard infrastructure is an example of how an availability risk factor affects the risks above it in the pyramid. Availability risk increases because it is difficult to ensure that all equipment is properly maintained and that the enterprise has skills to fix each type of equipment should it fail. Access risk increases because security patching is difficult with a diverse set of server types and access controls are difficult when users have many different passwords. Accuracy risk increases because of the need to manually integrate data across disparate systems. Finally, agility risk increases because existing applications are difficult to extend or convert, thus reducing organizational agility.

### *Where to Start with Risk Management*

The pyramid provides a map for addressing the complexity of IT risks. Factors at the base of the pyramid provide the greatest "bang for the buck" in an enterprise with limited resources. First, correcting availability and access risk factors can often be cost-justified, whereas it can be more difficult to compute an ROI on accuracy and agility factors such as standard business processes or automated systems interfaces. Second, even when cost-savings are not readily apparent, business executives can immediately grasp the business impacts of losing sensitive data or losing their systems for a day. They may be willing to invest in "insurance" activities to reduce these risks quickly. Lastly, factors at the base of the pyramid typically require less business involvement than factors at the top. Less negotiation and organizational change is required to implement configuration controls, patch management, or IT skills improvements than to restructure applications or change the IT/Business relationship.

By focusing at the base of the pyramid, IT executives can start on the long-term task of resolving accuracy and agility risks, while achieving "quick hits" that give demonstrable value for availability and access risks along the way. For example, Tektronix, a $2Billion electronics manufacturer, found that it could not divest a business unit because its systems were too intertwined with two other business units. This agility risk arose because for decades, they had incrementally patched core systems to meet new requirements rather than building new systems or re-architecting old ones. The result was that key financial and manufacturing processes for three business units snaked through a hodgepodge of infrastructure and applications with little to no documentation or standardization. Quarterly financial closes took several weeks, credit approvals required 24 hours, and expediting an order typically required five separate phone calls.

Tektronix had already begun to resolve these issues three years earlier by consolidating seven data centers into one, four computing platforms into two (with mainframes outsourced separately), and a variety of communications protocols into a single IP-based network. This reduced the firm's availability risk and laid the foundation for additional transformation. Only then could the CFO and CIO begin a $40-million, three-year initiative to redesign processes and replace legacy applications through a new ERP. They started with a single division to create uniform global processes, and then integrated the other two business units in a standard, well-documented way.

Today, accuracy risk is much lower, as evidenced by higher inventory visibility, lower days sales outstanding, faster credit approvals, and a five-fold increase in the percentage of same-day shipments. Furthermore, agility risk decreased, as the firm was able to sell a business unit easily, was able to integrate a new acquisition in less than 60 days, and had better information visibility to make strategic decisions. By starting at the bottom of the pyramid and working upwards, Tektronix reduced all four IT risks.

### *What If We Can't Wait to Address Integrity or Strategic Change Risks?*

Risk factors at the top of the pyramid tend to require long-term collaborative solutions involving IT and the business. IT executives can begin working on these long-term solutions at the same time that they address lower-tier risks. However, they need to recognize that higher-tier risks cannot be fully resolved without addressing the lower-tier risk factors. For example, executives can begin the long process of improving the IT/business relationship by implementing transparent metrics and oversight.[2] However, during this process, they should also work on availability and access risk factors such as IT staffing shortages and configuration controls. Otherwise, continuing risks in availability and access may undo any benefits from increased transparency.

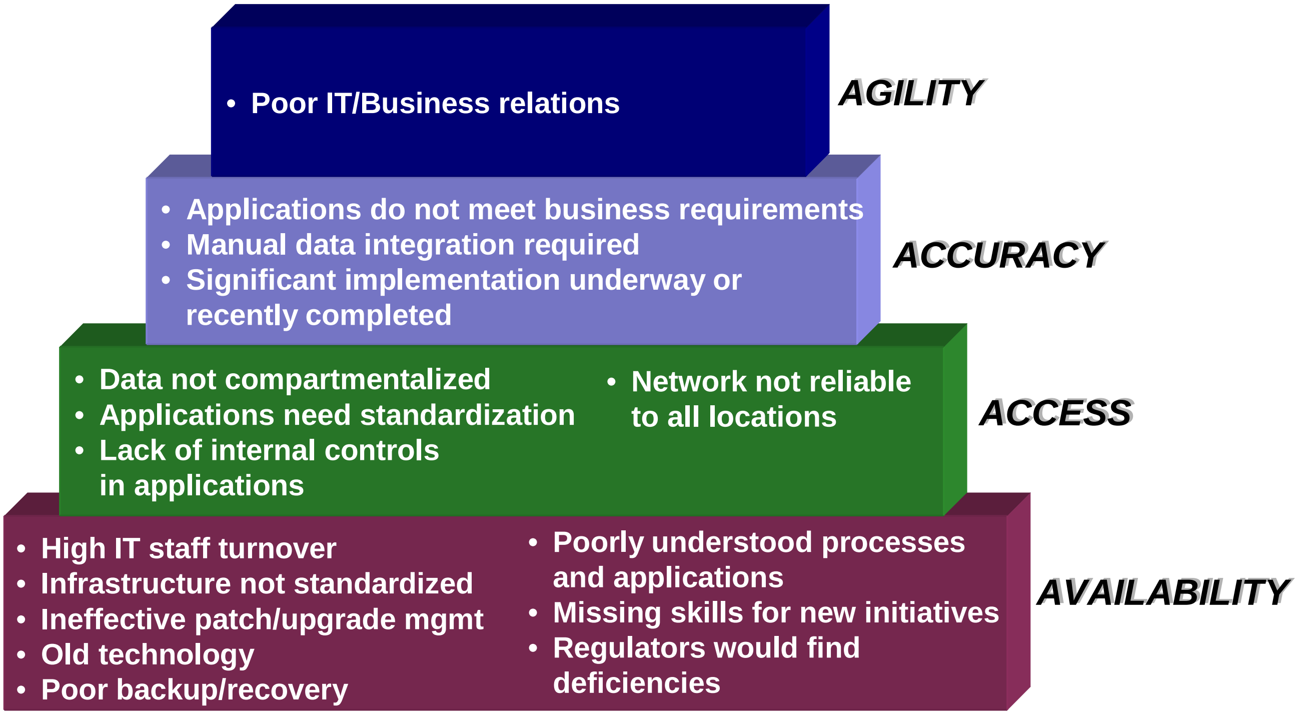
[2] See *What Are the Key Capabilities of Effective CIOs?* MIT Sloan CISR Research Briefing Vol. IV, No. 3C, October 2004.

Addressing an accuracy or agility risk without addressing foundational availability and access risk factors leads to short-term solutions that need to be reworked later. For example, many firms are addressing immediate Sarbanes-Oxley accuracy issues by using data warehouses to integrate disparate financial systems. These stopgap measures will ultimately need to be replaced when the firms are better able to document processes, improve internal controls, and standardize infrastructure and processes. Worse still, the next requirement (e.g., new privacy legislation, etc.) may require another stopgap solution.

### *Conclusion*

The risk pyramid charts a path through the complexity of IT risk management. IT executives should start risk management by resolving factors associated with availability and access. Reducing these risks pays immediate benefits to the enterprise, and also provides a foundation for the more difficult challenges of reducing accuracy and agility risks.

**Figure 1: The IT Risk Pyramid**



• Poor IT/Business relations
AGILITY
• Applications do not meet business requirements
• Manual data integration required
• Significant implementation underway or recently completed
ACCURACY
• Data not compartmentalized
• Applications need standardization
• Lack of internal controls in applications
• Network not reliable to all locations
ACCESS
• High IT staff turnover
• Infrastructure not standardized
• Ineffective patch/upgrade mgmt
• Old technology
• Poor backup/recovery
• Poorly understood processes and applications
• Missing skills for new initiatives
• Regulators would find deficiencies
AVAILABILITY

Analysis of 134 surveys shows that risk factors for a given enterprise IT risk (level of the pyramid) are statistically significantly correlated with amount of not only that risk, but also one or more risks above it in the pyramid.

Center for Information Systems Research
Sloan School of Management
Massachusetts Institute of Technology
RESEARCH BRIEFING
MITSloan MANAGEMENT

Volume V Number 3B December 2005

# What Makes an IT Risk Management Process Effective?

**George Westerman,** *Research Scientist*
*MIT Center for Information Systems Research*

The causes and effects of IT risk are complex, especially in large organizations. Only a well-defined risk management process can make sense of the complexity. According to Novartis CIO James Barrington:

> *"The organization is so complex—we've grown to 75,000 PCs with thousands of servers, all sorts of security issues—there's not a physical way to manage all of the risk associated with such a large environment in a perfect way. So, we've taken the approach that if you can't eliminate the risk, better try and understand it and manage it.*
>
> *So, we have started trying to understand the risk in each of these areas. And once we know the risk, then we try and manage the solution or the effort in direct relation to the size of the risk… That's very helpful for us… we get a much better leverage on our resources."*

## *The IT Risk Management Process*

The IT Risk Management process is simultaneously distributed and centralized (Figure 1). Experts in each part of the enterprise identify and assess risks in their areas. These local risk managers address each risk they control, and escalate large risks (or risks that require action by other people) to managers with broader authority.

The process provides a global view of all risks in a domain (see Figure 2) so managers can make tradeoffs and prioritize limited resources to shape an acceptable risk profile. Managers can choose to address each risk in one of four ways:

- *Avoid* the risk, by either stopping an activity or deciding not to undertake a risky activity.
- *Transfer* the risk, such as by outsourcing a process or buying insurance.
- *Reduce* the risk, by taking action to improve a risky condition.
- *Accept* the risk, either because the risk is small or because it cannot be addressed given current conditions and resources.

## *Effective Practices for the Risk Management Process*

Using survey data from more than 130 enterprises around the world, and interviews with more than 30, we have identified a set of practices that form the core of an effective IT risk management process.[1] Organizations with effective IT risk management:

1. Create the environment for risk management using:

   ***Risk Policies:*** Policies describe acceptable standards and unacceptable behaviors in all risk-relevant processes. Examples include infrastructure standards, e-mail retention policies, vendor management rules and information privacy protections. Clear, well-publicized policies help risk managers in each area identify risky conditions, and help employees throughout the enterprise avoid inappropriate behaviors or decisions.

   ***Best Practices:*** Industry "best practices," such as recommended software configurations, daily virus updates and standard internal controls, are often available from industry specialists and trade associations. Best practices enable risk managers to reliably implement a baseline of "good enough" risk protection in standard areas. Then, effective risk managers can focus on unique processes that need more attention.

2. Ensure a consistent view across multiple units and functions using:

   ***Formal Risk Categories:*** A small but comprehensive set of well-defined categories for IT risks and risk factors improves the risk management process in two ways. First, the categories

[1] Organizations using each of these practices reported mitigating statistically significantly more risk in at least three of four enterprise IT risks: availability, access, accuracy, and agility. For more information on these four risk categories, see *Understanding the Enterprise's IT Risk Profile*, MIT Sloan CISR Research Briefing Vol IV, No 1C, March 2004.

and their definitions serve as a checklist to help local experts identify and assess risks. Second, they help higher levels of the organization prioritize and monitor risks by grouping similar risks across the enterprise.

***Risk Register:*** An IT risk register records and tracks all IT risks. At a minimum the risk register identifies the name and description of the risk, category, risk owner and the risk's impact and likelihood. The register also tracks what action is planned, and whether progress is being made.

***Quantified Risk Assessments:*** Quantified assessments of risk impact and likelihood improve the firm's ability to globally compare and prioritize risks. Because of its newness and complexity, IT risk does not have the detailed actuarial information that insurance companies use to price other types of risk— IT risk managers must use less precise methods to assess IT risk. Some assess each risk's impact and likelihood broadly, using well-defined thresholds for high, medium and low. Others use more detailed scoring sheets to generate relative impact and likelihood scores based on heuristics and best practices.

3. Provide the correct resources for the process, including:

   ***Single person in charge of process:*** The chief IT risk manager designs and runs the risk management process but does not manage particular risks. The process enables local experts to identify and address IT risks, and higher-level managers to monitor and prioritize important ones. By making a single person accountable for the process, effective firms gain a clear focus on IT risk management and a mechanism for continuous improvement.

   ***Risk committee:*** An IT risk committee, consisting of senior IT and business executives, makes decisions on how to address the most important IT risks facing the enterprise. The committee also considers changes such as adding new IT risk categories, conducting audits or threat assessments or adjusting the firm's acceptable risk profile.

### *Improving the Process Over Time*

The risk management process typically requires 12–18 months to reach a baseline level of effectiveness. During this learning period, the process can be difficult. People throughout the organization learn how to identify and assess risks, and become comfortable sharing risk information. Additionally, the chief risk manager continuously monitors and improves the process to meet business needs without being overly burdensome. For example, the first cycle of the IT risk management process in one financial services firm identified more than 300 risks—too many to meaningfully prioritize or monitor. Through an iterative process of discussion and policy improvement, the firm reduced the number of active IT risks to around 30.

Risk managers monitor risk trends—using charts like Figure 3 or regular updates to a risk map as shown in Figure 2—to ensure that the organization is focused on the correct risks and that new risks are being addressed effectively. In time, instead of repeatedly conducting detailed assessments of all risks, firms can shift to incremental status updates on existing risks coupled with targeted new risk assessments. In addition, many new risks can be identified by embedding risk management into other IT processes. For example, several firms have embedded risk-related reviews into IT project initiation and review processes, so that risks are identified or avoided as part of the normal demand management process.

### *Benefits of an Effective IT Risk Management Process*

Upon accepting the new CIO position at financial services provider PFPC, Michael Harte decided to make IT risk management a key pillar of his transformation program.[2] He and his staff developed an IT risk management process to guide key IT governance decisions and improve the firm's IT risk profile. Harte now participates in sales calls in order to showcase the firm's IT risk management capabilities to potential clients.

Although not all CIOs would gain similar customer attention for their IT risk management processes, the other benefits are clear. Firms using the practices listed above report statistically significantly lower risk, higher confidence in their risk management capabilities and less likelihood that the enterprise is missing important IT risks. The benefits also go beyond risk avoidance. Discussing IT decisions in terms of specific risk/return tradeoffs puts technical decisions into language that business executives are comfortable with. This transparency improves the relationship between IT and business by making risk-related decisions easier and clarifying the importance of key IT governance processes.

[2] See MIT Sloan CISR Working Paper No. 352, *PFPC: Building an IT Risk Management Competency* by George Westerman and Robert Walpole, April 2005.

**Figure 1: The IT Risk Management Process Balances Local Expertise with Central Oversight**

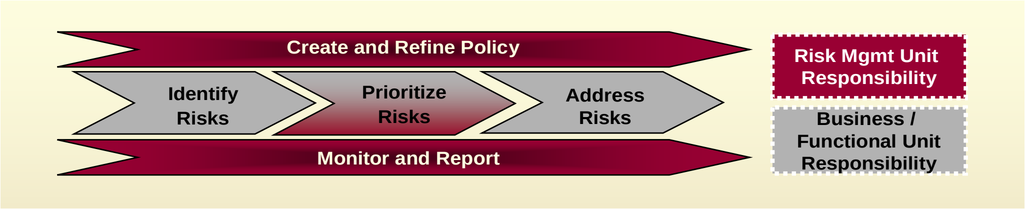


**Figure 2: The IT Risk Map Provides a Global View for Prioritization and Monitoring**

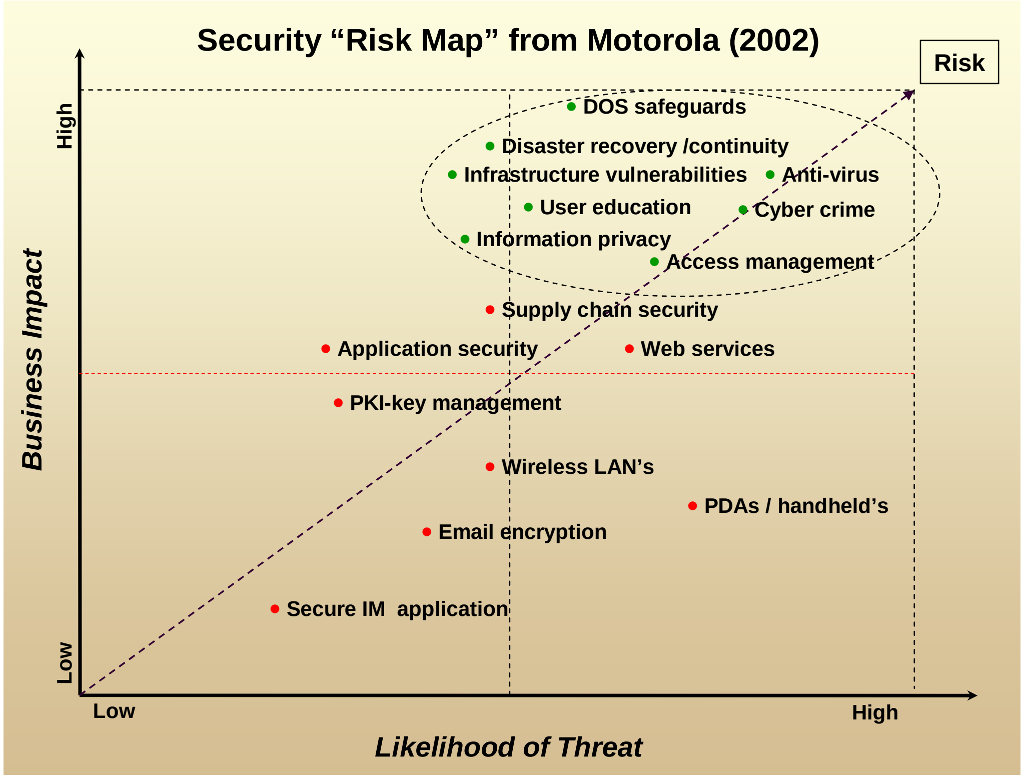
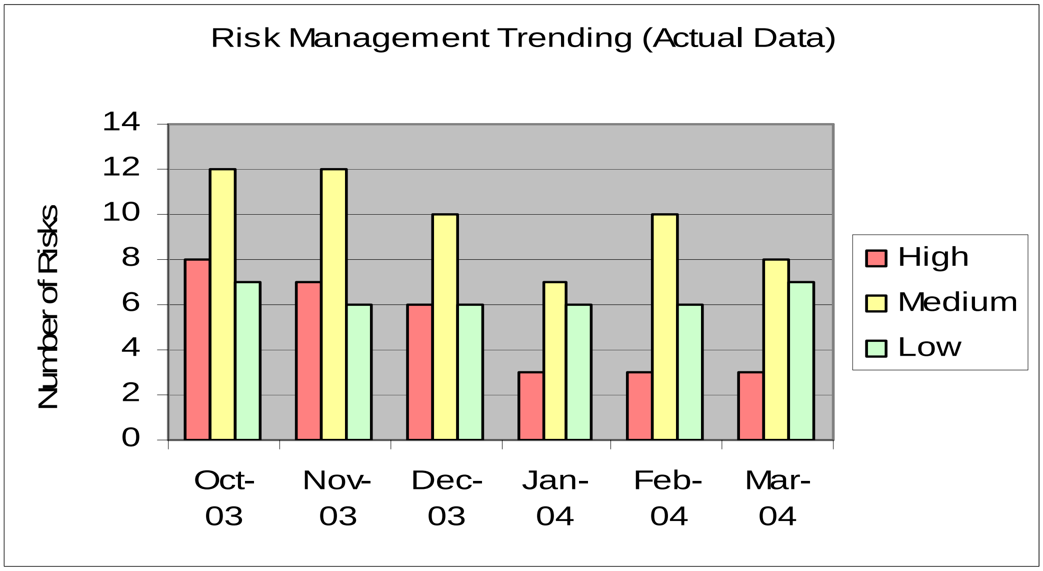


**Figure 3: Regular Monitoring Ensures that the Most Important Risks Are Being Addressed First**



## *About the Center for Information Systems Research*

### CISR MISSION

CISR was founded in 1974 and has a strong track record of practice based research on the management of information technology. As we enter the twenty-first century, CISR's mission is to perform practical empirical research on how firms generate business value from IT. CISR disseminates this research via electronic research briefings, working papers, research workshops and executive education. Our research portfolio includes:

- Effective IT Oversight
- The Future of the IT Organization
- An IT Manifesto for Business Agility
- Business Models and IT Investment & Capabilities
- IT-Enabling Business Innovation
- Effective Governance Outsourcing
- IT Engagement Models and Business Performance
- Effective IT Governance
- Enterprise Architecture as Strategy
- IT Portfolio Investment Benchmarks & Links to Firm Performance
- IT-Related Risk
- IT-Enabled Business Change

Since July 2000, CISR has been directed by Peter Weill, formerly of the Melbourne Business School. Drs. Jeanne Ross, George Westerman and Nils Fonstad are full time CISR researchers. CISR is co-located with MIT Sloan's Center for e-Business and Center for Coordination Science to facilitate collaboration between faculty and researchers.

CISR is funded in part by Research Patrons and Sponsors and we gratefully acknowledge the support and contributions of its current Research Patrons and Sponsors.

### CONTACT INFORMATION

Center for Information Systems Research
MIT Sloan School of Management
3 Cambridge Center, NE20-336
Cambridge, MA 02142
Telephone: 617/253-2348
Facsimile: 617/253-4424
http://web.mit.edu/cisr/www

| | |
|---|---|
| Peter Weill, Director | pweill@mit.edu |
| Chris Foglia, Center Manager | cfoglia@mit.edu |
| David Fitzgerald, Asst. to the Director | dfitz@mit.edu |
| Jeanne Ross, Principal Res. Scientist | jross@mit.edu |
| George Westerman, Res. Scientist | georgew@mit.edu |
| Nils Fonstad, Research Scientist | nilsfonstad@mit.edu |
| Jack Rockart, Sr. Lecturer Emeritus | jrockart@mit.edu |
| Chuck Gibson, Sr. Lecturer | cgibson@mit.edu |
| CISR Administrative Assistant | cisr-aa@mit.edu |

### CISR RESEARCH PATRONS

BT Group
The Boston Consulting Group, Inc.
Diamond Management & Technology Consultants
Gartner
Hewlett-Packard Company
IBM Corporation
Microsoft Corporation
Tata Consultancy Services—America

### CISR SPONSORS

Aetna Inc.
Allstate Insurance Co.
American Express Corp.
AstraZeneca Pharmaceuticals, LP
Banco ABN Amro Real S.A.
Biogen Idec
Campbell Soup Company
CareFirst BlueCross BlueShield
Care USA
Celanese
Chevron Corporation
Chubb & Sons
Det Norske Veritas (Norway)
Direct Energy
eFunds Corporation
EMC Corporation
Family Dollar Stores, Inc.
The Guardian Life Insurance Company of America
Information Services International
ING Groep N.V.
Intel Corporation
International Finance Corp.
Merrill Lynch & Co., Inc.
MetLife
Mohegan Sun
News Coporation
Nissan North America, Inc.
Nomura Research Institute, Ltd.
Northrop Grumman Corp.
Owens Corning
PepsiAmericas, Inc.
Pfizer, Inc.
PFPC, Inc.
Quest Diagnostics
Raytheon Company
Standard & Poor's
State Street Corporation
TD Banknorth
Telenor ASA (Norway)
Time Warner Cable
Trinity Health
TRW Automotive, Inc.
Unibanco S.A.
United Nations — DESA
US Federal Aviation Administration
The Walt Disney Company

MITSloan
MANAGEMENT