Communications of the Association for Information Systems

Volume 25 Article 41

12-1-2009

Developments in Practice XXXIII: A Holistic Approach to Managing IT-based Risk

Heather A. Smith
Queen's School of Business, Queen's University at Kingston, hsmith@business.queensu.ca

James D. McKeen
Queen's School of Business, Queen's University at Kingston

Follow this and additional works at: https://aisel.aisnet.org/cais

Recommended Citation
Smith, Heather A. and McKeen, James D. (2009) "Developments in Practice XXXIII: A Holistic Approach to Managing IT-based Risk," *Communications of the Association for Information Systems*: Vol. 25 , Article 41.
DOI: 10.17705/1CAIS.02541
Available at: https://aisel.aisnet.org/cais/vol25/iss1/41

This material is brought to you by the AIS Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in Communications of the Association for Information Systems by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

www.manaraa.com

Communications of the Association for Information Systems

CAIS

Developments in Practice XXXIII: A Holistic Approach to Managing IT-based Risk

Heather A. Smith

Queen's School of Business, Queen's University at Kingston, Canada

hsmith@business.queensu.ca

James D. McKeen

Queen's School of Business, Queen's University at Kingston, Canada

Abstract:

Not long ago, IT-based risk was a fairly low-key activity focused on whether IT could deliver projects successfully and keep applications up and running. But with the opening up of the organization's boundaries to external partners, service providers, external electronic communications, and online services, managing IT-based risk has morphed into a "bet the company" proposition. Not only is the scope of the job bigger, the stakes are much higher. As companies have become more dependent on IT for everything they do, the costs of service disruption and inadequate security practices have escalated exponentially. Therefore, the job of managing IT-based risk has become broader and more complex. Whereas in the past companies have sought security through physical or technological means (e.g., locked rooms, virus scanners), there is now growing understanding that managing IT-based risk must be a strategic and holistic activity that is not just the responsibility of a small group of IT specialists, but part of a mindset that extends from partners and suppliers to employees and customers. This paper explores how organizations are addressing and coping with increasing IT-based risk. It presents the results of an in-depth discussion of this issue with 20 senior IT practitioners and the challenges facing them. It proposes a holistic view of risk and examines the characteristics and components needed to develop an effective risk management framework, presenting a generic framework for integrating the growing number of elements involved in it. Finally, it describes successful practices organizations could use for improving their risk management capabilities.

Keywords: risk management, enterprise risk, risk framework, risk sources, risk management capabilities, external risk, internal risk

Volume 25, Article 41, pp. 519-530, December 2009

Communications of the Association for Information Systems

I. INTRODUCTION

It's another one of those dramatic "paradigm shifts" for which IT is famous. Not so long ago, IT-based risk was a fairly low-key activity focused on whether IT could deliver its projects successfully and keep its applications up and running [McKeen and Smith 2003]. But with the opening up of the organization's boundaries to external partners and service providers, external electronic communications, and online services, managing IT-based risk has morphed into a "bet the company" proposition. Not only is the scope of the job bigger, the stakes are much higher. As companies have become more dependent on IT for everything they do, the costs of service disruption have escalated exponentially. Now, when a system goes down, the company effectively stops working and customers cannot be served. And criminals routinely seek ways to wreak havoc with company data, applications, and websites. New regulations to protect privacy and increase accountability have also made executives much more sensitive to the consequences of inadequate IT security practices—either internally or from service providers. Finally, the risk of losing or compromising company information has risen steeply. No longer are a company's files locked down in a glass house or accessible only by company staff. Today there are literally hundreds of ways company information can be exposed to the public. Our increasing mobility, the portability of storage devices, and the growing sophistication of cyber-threats are just a few of some of the more noteworthy.

Therefore, the job of managing IT-based risk has become much broader and more complex. It is now widely recognized as an integral part of any technology-based work—no matter how minor. As a result, many IT organizations have been given the responsibility of not only managing risk in their own activities (i.e., project development, operations, and delivering business strategy), but also of managing IT-based risk in *all* company activities (e.g., mobile computing, file sharing, and online access to information and software). Whereas in the past companies have sought to achieve security through physical or technological means (e.g., locked rooms, virus scanners), there is now growing understanding that managing IT-based risk must be a strategic and holistic activity that is not just the responsibility of a small group of IT specialists, but part of a mindset that extends from partners and suppliers to employees and customers.

To explore how organizations are addressing and coping with increasing IT-based risk, the authors convened a day-long focus group of twenty senior IT managers from a number of organizations in a variety of industries. In preparation for this meeting, they were asked to consider several questions about how they identified and managed IT-based risk and to prepare a short presentation to be shared with the group. These included questions about categories of IT-based risk; whether their firm had an IT-based risk management strategy; different levels of risk; and skills, practices, tools, and roles for managing risk. Several participants also provided the authors with copies of methodologies, checklists, and policies used by their organizations to identify and manage IT-based risk.

This paper presents the results of this in-depth discussion, combined with relevant practitioner and academic literature. It first looks at the challenges facing IT managers in the arena of risk management and proposes a holistic view of risk. Next it examines some of the characteristics and components needed to develop an effective risk management framework and presents a generic framework for integrating the growing number of elements involved in it. Finally, it describes some successful practices organizations could use for improving their risk management capabilities.

II. A HOLISTIC VIEW OF IT-BASED RISK

With the explosion of new IT-based risks facing organizations in the past decade, there is an increasing recognition that risk means more than simply "the possibility of a loss or exposure to loss" [Mogul 2004] or even a hazard, uncertainty, or opportunity [McKeen and Smith 2003]. Today, "risk" is a multilayered concept which implies there is much more at stake.

> *IT risk has changed. IT risk incidents harm constituencies within and outside companies. They damage corporate reputations and expose weaknesses in companies' management teams. Most importantly, IT risk dampens an organization's ability to compete* [Hunter and Westerman 2007].

As a result, companies are beginning to talk about "enterprise risk management" as a more comprehensive and integrated approach to dealing with risk [Slywotzky and Drzik 2005]. While not every risk affecting an enterprise will be an IT-based risk, agreed the focus group, the fact remains that a large number of the risks affecting the

enterprise have an IT-based component. For example, one firm's IT Risk Management Policy notes that the goal of risk management is to ensure that technology failures or data integrity do not compromise the company's strategic objectives, the company's reputation and stakeholders, or its success and reputation.

This heightened sensitivity to IT-based risk has even reached many boards of directors.

> *Ever since the Y2K scare, boards have grown increasingly nervous about corporate dependence on information technology…. [However,] few understand the full degree of their operational dependence … [and] lack the fundamental knowledge needed to ask intelligent questions about… IT risk…. This leaves CIOs… pretty much on their own [*Nolan and McFarlan 2005].

Thus, in spite of the increasing number and complexity of IT-based threats facing organizations, it is still very difficult to get senior business leaders to give the attention (and the resources) needed to effectively manage them. A recent global survey noted, "while the security community recognizes that information security is part of effective *business* management, managing information security risk is still overwhelmingly seen as an IT responsibility worldwide" [Berinato 2007]. In short, while IT has become increasingly central to business success, many enterprises have not yet adjusted their processes to incorporate IT-based risk management [Hunter and Westerman 2007].

Knowing what's at stake, risk management is perennially in the top ten priorities for CIOs [Hunter et al. 2005], and efforts are being made to put effective capabilities and processes in place in IT organizations. However, only 5 percent of firms are at a high level of maturity in this area and most (80 percent) are still in the initial stages of this work [Proctor 2007]. Addressing risk in a more professional, accountable, and transparent fashion is an evolution from traditional IT security work. At a recent Gartner symposium, it was pointed out that:

> *… traditionally, [IT] security has been reactive, ad hoc, and technically-focused…. The shift to risk management requires an acceptance that you can't protect yourself from everything, so you need to measure risk and make good decisions about how far you go in protecting the organization* [Proctor 2007].

Focus group companies largely reflected this transitional state. "Information security is a primary focus of our risk management strategy," said one manager. "It's very, very visible, but our business has yet to commit to addressing risk issues." Another stated, "we have a risk management group focused on IT risk, but lots of other groups focus on it too…. As a result, there are many different and overlapping views, and we are missing integration of these views." "We are constantly trying to identify gaps in our risk management practices and to close them," said a third.

There is, however, no hesitation about identifying the sources of risk. Every company in the group had its own checklist of risk items, and the experts have developed several different frameworks and categorizations which aim to be comprehensive (see Appendix A for an overview of some common frameworks in use today). What everyone agrees on is that any approach to dealing with IT-based risk must be holistic—even though it is an "onerous" job to package it as a whole. "Every category of risk has a different vocabulary," explained one focus group manager. "Financial, pandemic, software, information security, disaster recovery planning, governance, and legal—each view makes sense but pulling them together is very hard." Risk is often managed in silos in organizations, resulting in uncoordinated approaches to its management and to decision-making incorporating risk [Mogul 2004]. This is why many organizations, including several in the focus group, are attempting to integrate the wide variety of issues involved into one holistic enterprise risk-management strategy that uses a common language to communicate [Slywotzky and Drzik 2005; Mogul 2004; Nolan and McFarlan 2005].

The connection between all of the different risk perspectives is the enterprise. Any IT problem that occurs—whether with an application, a network, a new system, a vendor or a hacker (to name just a few)—has the increasing potential to put the enterprise at risk. Thus, a holistic view of IT-based risk must put the enterprise front and center in any framework or policy. A risk to the enterprise includes anything (either internal or external) that affects its:

- Brand
- Reputation
- Competitiveness
- Financial value
- End state (i.e., its overall effectiveness, efficiency and success)

Figure 1 offers an integrated, holistic view of risk from an enterprise perspective.

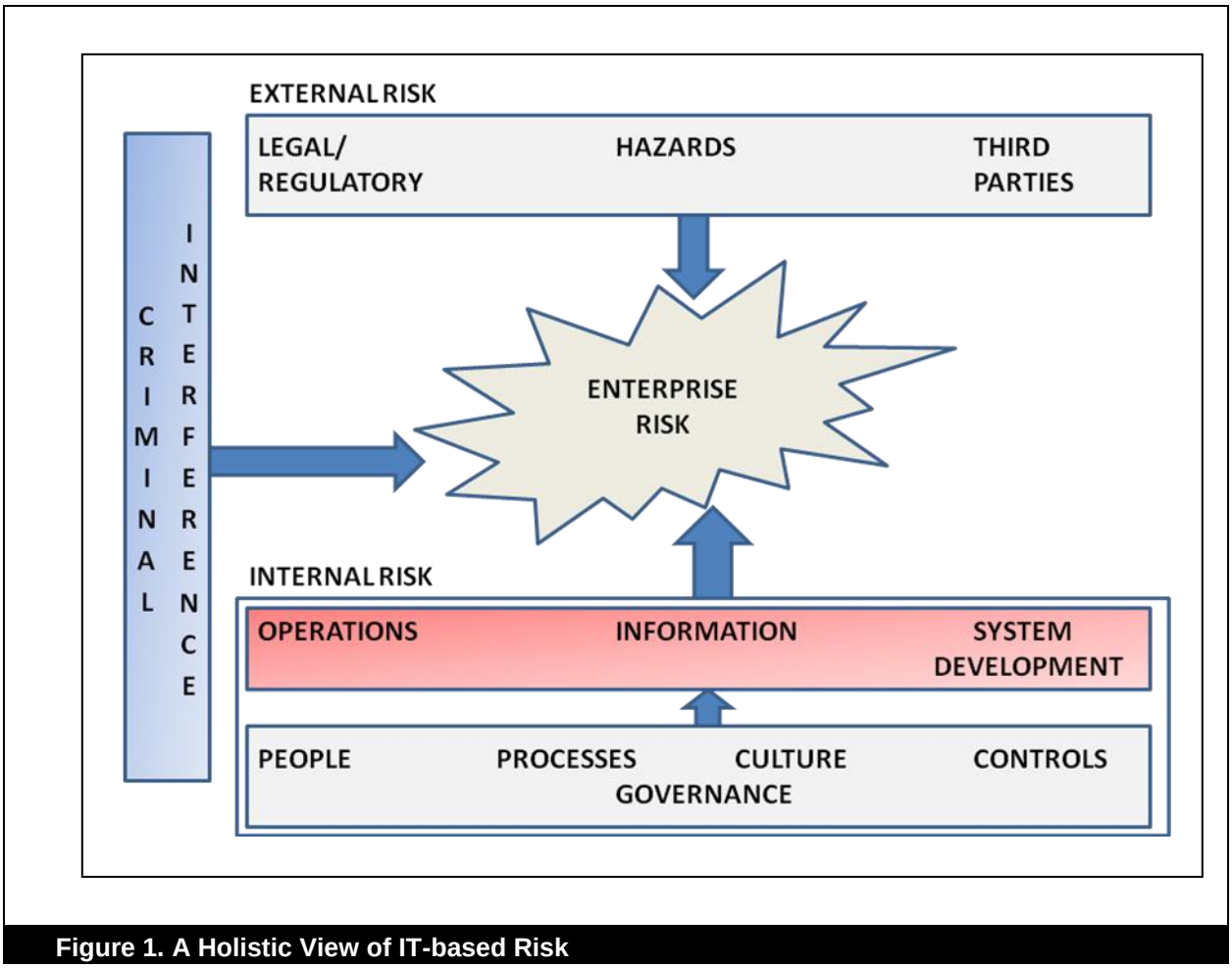

Figure 1. A Holistic View of IT-based Risk

There are a wide variety of both internal and external IT-based risks that can affect the enterprise. *Externally,* risks can come from:

- **Third parties** such as partners, software vendors, service providers, suppliers, or customers
- **Hazards** such as disasters, pandemics, geopolitical upheavals, or environmental considerations
- **Legal and regulatory issues**, i.e., failure to adhere to the laws and regulations affecting the company, such as privacy, financial reporting, environmental reporting, and e-discovery

Internally, some risks are well-known, such as those traditionally associated with IT operations (availability, accessibility) and systems development (not meeting schedules or budgets or delivering value). Others are newer and, while they must be managed from within the organization, they may include both internal and external components. These include:

- **Information risks**, such as those affecting privacy, quality, accuracy, protection
- **People risks**—those caused by mistakes or lack of adherence to security protocols
- **Process risks**—problems caused by poorly-designed business processes or by failure to adapt business processes to IT-based changes
- **Cultural risks**, including risk aversion as well as lack of risk awareness
- **Controls**—ineffective or inadequate controls to prevent or mitigate risk incidents
- **Governance**—ineffective or inadequate structure, roles, or accountabilities to make appropriate risk-based decisions

Finally, there is the risk of *criminal interference*, either from inside or outside the organization. Unlike other types of risk, which are typically inadvertent, criminal actions are deliberate attacks on the enterprise, its information, or sometimes its employees or customers. Such threats are certainly not new. Everyone is familiar with viruses and hackers. What *is* new, however, is that there are many more groups and people targeting organizations *and* individuals. These include other national governments, organized crime, industrial spies, and terrorists. "These people are not trying to bring systems down, like in the past," explained one focus group member. "They are trying to get information."

Holistic Risk Management: A Portrait

Figure 2. Dora Maar with Cat by Picasso

Tackling risk in a holistic fashion is challenging and building an effective framework for its management will not occur overnight. It is, therefore, important to keep the big picture in mind or the process could degenerate into overwhelming bureaucracy. It is interesting to note that there is much more agreement from both the focus group and other researchers about what effective risk management *looks like* than *how* to do it. This section, therefore, presents an impressionist portrait of what constitutes holistic risk management in order to show what this big picture should portray. While a closer look at the detailed elements composing this picture will also be needed, it is essential that all people and functions involved in risk management agree on what image is being created. Otherwise, if one person is trying to create a Picasso while another is painting "Whistler's Mother," it is unlikely that the resulting portrait will be pleasing to anyone!

With this in mind, we sketch some of the characteristics and components of a portrait of effective, holistic risk management:

Figure 3. Whistler's Mother by J.M. Whistler

1. **Focus on What's Important.** "Risks are inevitable," admitted a focus group manager. "The first question we must ask is: 'What are we trying to protect?'" said one manager. "There's no perfect package, and some residual risk must always be taken." Another added, "… risks are inevitable, but it's how they're managed—our response, contingency plans, team readiness, and adaptability—that makes the difference." In short, risk is uncertainty that *matters,* something that can hurt or delay an enterprise from reaching its objectives [Hillson 2008]. While many managers recognize that it's time to take a more strategic view of risk, "we still don't have our hands around what's important and what we should be monitoring and protecting" [Berinato 2007]. Risk management is, therefore, not about anticipating *all* risks, but about attempting to reduce *significant* risks to a manageable level [Austin and Darby 2003] and knowing how to assess and respond to it [Slywotzky and Drzik 2005]. Yet, more than protecting the enterprise, risk management should also enable it to take *more* risk in the safest possible way [Caldwell and Mogull 2006]. Thus, the focus of effective risk management should not be about saying "no" to a risk, but how to say "yes," thereby building a more agile enterprise [Caldwell and Mogull 2006].

2. **Expect the Image to Change Over Time.** Few companies really have a good grasp of risk management because it is a discipline that is evolving rapidly [Proctor 2007]. As a result, it would be a mistake to codify risk practices and standards too rapidly, according to the focus group. Efforts to do this have typically resulted in "paperwork without context," said one manager. Within a particular risk category, risk management actions should be "continuous, iterative, and structured," the group agreed. In recognition of this reality, most focus-group organizations have a mandatory risk assessment at key stages in the system development process to capture the risk picture involved with a particular project at several points in time, and many have regular, ongoing reviews of required operational controls on an annual or biannual basis to do the same thing. In addition, when incidents occur, there should always be a process for evaluating what happened, assessing its impact and determining if controls or other management processes need to be adapted [Coles and Moulton 2003]. Finally, organizations should also be continually attempting to simplify and streamline controls wherever possible to minimize their burden. This is a process that is often missed, admitted one manager.

However, while each of these steps is useful in keeping one aspect of the risk picture in mind, it is also essential to stand back from these initiatives and see how the whole image is developing. It is this more strategic and holistic view that is often missing in organizations and which firms often fail to communicate to their staff. One of the greatest risks to organizations comes from employees themselves, not necessarily through their intentional actions, but because they don't recognize the risks involved in their actions [Berinato 2007]. Therefore, many believe it is time to recognize that risk cannot be managed solely through controls, procedures, and technology, but that all employees must understand the concepts and goals of risk management because the enterprise will always need to rely on their judgment to some extent [Symantec 2007]. In the same vein, many managers also need to better understand this risk picture because they frequently do not comprehend the size and nature of the risks involved and thus resource their management inappropriately [Coles and Moulton 2003]. As a result they tend also to delegate many aspects of risk management to lower levels in the organization, thus preventing the development of any longer term, overall vision [Witty 2008; Proctor 2008].

3. **View Risk from Multiple Levels and Perspectives.** Instead of dealing with security "incidents" in a one-at-a-time manner, focus group members are trying to do a better job of root-cause analysis and understanding risks in a more multifaceted way. To date, risk management has tended to focus largely on the operational and tactical levels, but they suggest that risk management should also be viewed in a strategic way. A focus group manager explained, "we need to assess risk trends and develop strategies for dealing with them. Tactics for dealing with future threats will then be more effective and easier to put in place." Another manager noted: "we must aim for redundancy of protection; that is, multiple layers, to ensure that if one layer fails, others will catch any problems."

Furthermore, risk, security, and compliance are often intermixed in people's minds. While each of these is a valid lens through which to view risk, the challenge comes when they are seen as being the same thing. For example, one expert noted that 70 percent of a typical "security" budget is spent on compliance matters, not on protecting and defending the organization [Society for Information Management 2008], and this imbalance means that overall spending in many firms is skewed. One focus group firm uses the "prudent person" rule to deal with risk, which recommends a diversity of approaches—proactive, prevention, due diligence, credibility, and promoting awareness—to ensure that it is adequately covered and that all stakeholders are properly protected. Monitoring and adapting to new international standards and laws, completing overall health checks, and analysis of potential risks are other new dimensions of risk that should be incorporated into a firm's overall approach to risk management.

Developing a Risk Management Framework

With the big picture in mind, organizations can begin to develop a framework for filling in the details. The objective of a risk management framework (RMF) is to create a common understanding around risk, to ensure that the right risks are being addressed at the right levels and to involve the right people in making risk decisions. It also serves to guide the development of risk policies and integrate appropriate risk standards and processes into existing practices (e.g., the SDLC). No company in the focus group had yet developed a comprehensive framework for addressing IT-based risk, although many had significant pieces in place or in development. In this section, we attempt to piece these together to sketch out what an RMF might contain.

An RMF should serve as a high level overview of how risk is to be managed in an enterprise; it can also act as a structure for reporting on risk at various levels of detail. Many of the focus group companies have created risk management policies to guide staff as to how IT risk and security are to be treated and require all staff to read and sign them. Unfortunately, they are typically so long and complex as to be overwhelming and ineffective. "Our security policy alone is 200 pages. How enforceable is it?" complained a focus group manger. Another noted that the language in his company's policy was highly technical. As a result, there was considerable user noncompliance in following the recommended best practices. Furthermore, there are often a plethora of committees, review boards, councils, and control centers, all designed to deal with one or more aspects of risk management, but which contribute to the general complexity of managing IT-based risk in an organization.

It should not be surprising that this situation exists, given the rapidity with which technologies, interfaces, external relationships, and dependencies have developed within the past decade. Organizations have struggled to simply keep up with the waves of legislation, regulation, globalization, standards, and transformation that seem to continually threaten to engulf them. An RMF is thus a starting point for providing an integrated, top-down view of risk, defining it, identifying those responsible for making key decisions about it, and mapping which policies and standards apply to each area. Fortunately, current technology makes it easy to offer multiple views and multiple levels of this information, enabling different groups or individuals to understand their responsibilities and specific policies in detail and see links to specific tools, practices, and templates, while facilitating different types of reporting to different stakeholders at different levels. By mapping existing groups, policies, and guidelines into an RMF, it is easier to see where gaps exist and where complexities in processes should be streamlined.

A basic RMF includes the following:

- **Risk Category.** The general area of enterprise risk involved (e.g. criminal, operations, third party, etc.)
- **Policies and Standards.** These state, at a high level, the general principles for guiding risk decisions and identify any formal corporate, industry, national, or international standards that should apply to each risk category.[1] For example, one focus group company's policy regarding people states in part:

  > *Protecting the integrity and security of client and corporate information is the responsibility of every employee. Timely and effective reporting of actual and suspected privacy incidents is a key component of meeting this responsibility. Management relies on the collective experience and judgment of its employees.*

  Another's regarding culture states: "We need to embed a risk management focus and awareness into all processes, functions, jobs, and individuals."

- **Risk Type.** Each type of risk associated with each category (e.g., loss of information, failure to comply with specific laws, inability to work due to system outages) needs to be identified. Each type should have a generic name and definition, ideally linked to a business impact. Identifying all risk types will take time and probably require much iteration, as "there are an incredible variety of specific risks" [Mogul 2004]. However, developing lists and definitions is a good first step [McKeen and Smith 2003; Hillson 2008; Baccarini et al. 2004] and is already a common practice among the focus group companies, at least for certain categories of risk.
- **Risk Ownership.** Each type of risk should have an owner, either in IT or in the business. As well, there will likely be several stakeholders who will be affected by risk-based decisions. For example, the principal business sponsor could be the owner of risk decisions associated with the development or purchase of a new IT system, but IT operations and architecture as well as the project manager will clearly be key stakeholders. In addition to specialized IT functions, such as IT security, audit and privacy functions in the business will likely be involved in many IT risk-based decisions. Owners and stakeholders should have clear responsibilities and accountabilities. In the focus group, some major risk types were owned by committees, such as an Enterprise Risk Committee, or the Internal Audit, Social Responsibility and Risk Governance Committee, or the Project Risk Review Council on which stakeholder groups were represented.
- **Risk Mitigation.** As an RMF is developed, each type of risk should be associated with controls, practices, and tools for addressing it effectively. These fall into one of two categories: compulsory and optional. The focus group stressed that overemphasis on mitigation can lead to organizational paralysis or hyper-risk sensitivity. Instead, participants stressed the role of judgment in "right-sizing" mitigation activities wherever possible. "Our technology development framework does not tell you what you *have* to do, but it does give you things to consider in each phase," said one manager. "We look first at the overall enterprise risk presented by a project," said another, "and develop controls based on our evaluation of the level and types of risk involved." The goal, everyone agreed, is to provide a means by which risks can be managed consistently, effectively, and appropriately.[2]
- **Risk Reporting and Monitoring.** This was a rather controversial topic in the focus group. Although everyone agreed it is important to make risk and its management more visible in the organization, tracking and reporting on risk has a tendency to make management highly risk averse. One manager said:

  > *We spent a year trying to quantify risks and developing a roll up report, but we threw it away because audit didn't understand it and saw only one big risk. This led to endless discussion and no confidence that IT was handling risk well. Now we use a very simple reporting framework presenting risk as high, medium, or low. This is language we all understand*.

There are definitely pressures to improve risk measurement [Proctor 2007], but, clearly, care must be taken in how these metrics are reported. For example, one company uses a variety of self-assessments to ensure that risks have been properly identified and appropriate controls put in place. However, as risk management procedures become better understood and more codified, risk reporting can also become more formalized. This is particularly the case at present with operational process controls and fundamental IT security, such as virus or intrusion detection.

1. Some international standards include: COSO (www.erm.coso.org); AS/NZS (www.riskmanagement.com.au); and OCG's M_o_R (www.ogc.gov.uk/guidance_management_of_risk.asp).
2. The National Institute of Standards and Technology's Special Publication 800-30 provides guidance on specific risk mitigation strategies (http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf).

Communications of the Association for Information Systems

However, risk monitoring is an ongoing process, because levels and types of risk are changing continually. Thus, an RMF should be a dynamic document as new types of risk are identified, business impacts are better understood, and mitigation practices evolve. "We need to continually monitor all categories of risk and ask our executives if the levels of risk are still the same," said a focus group member. It is clear that failure to understand *how* risks are changing is a significant risk in itself [Proctor 2007]. It is, therefore, especially important to have a process in place to analyze what happened when an unforeseen risk does occur. Unless efforts are made to understand the root causes of a problem, it is unlikely that effective mitigation practices can be put in place [Austin and Darby 2003].

Improving Risk Management Capabilities

Risk management is not yet at the stage where there are well-documented best practices or standards in most areas. However, the focus group identified several actions that could lead to the development of effective risk management capabilities:

- **Look beyond technical risk.** One of the biggest inhibitors of effective risk management is too tight a focus on technical risk, rather than business risk. A traditional security approach tends to exclude this, often focusing only on technical threats or specific systems or platforms.
- **Develop a common language of risk.** A clearer understanding of business risk requires all stakeholders—IT, audit, privacy, legal, business managers—to speak the same language and use comparable metrics—at least at the highest levels of analysis where the different types of risk need to be integrated.
- **Simplify the presentation.** Having a common approach to discussing or describing risk is very effective, said several focus group members. While the work that is behind a simple presentation may be complex, presenting too much complexity can be counterproductive. The most effective approaches are simple—a narrative, a dashboard, a "stoplight" report, or another graphic style of report.
- **Right size.** Risk management should be appropriate for the level of risk involved. More effective practices allow for the adaptation of controls, while ensuring that the decisions made are visible and the rationale is communicated.
- **Standardize the technology base.** This is one of the most effective ways to reduce risk, but it also one of the most expensive.
- **Rehearse.** Many firms now have an emergency response team in place to rapidly deal with key hazards. However, it is less common that this team actually rehearses its disaster recovery, business continuity, or other types of risk mitigation plans. One manager noted that live rehearsals are essential to reveal gaps in plans and unexpected risk factors.
- **Clarify roles and responsibilities.** With so many groups in the organization now involved in managing risk in some way, it is critical that roles and responsibilities be documented and communicated. Ideally, this should be in the context of an RMF, but, even if one is not in place, efforts should be made to document which groups in the organization are responsible for which types of enterprise risk.
- **Automate where appropriate.** As risk management practices become standardized and streamlined, automated controls begin to make sense. Some tools can be very effective, noted the focus group, provided they are applied in ways that facilitate risk management, rather than becoming an obstacle to productivity.
- **Educate and communicate.** Each organization has its own culture. Most need to work with staff, business managers, and executives to make them *more* aware of risk and the need to invest in its management. However there are some organizations, like one insurance company in the focus group, that are so risk-phobic that they need education to enable them to take on *more* risk. These companies could benefit from better understanding their "risk portfolio" of projects [Day 2007]. Such an approach can often help encourage companies to undertake more risky innovation initiatives with more confidence.

III. CONCLUSION

Organizations are more sensitized to risk than ever before. The economy, regulatory and legal environment, business complexity, the increasing openness of business relationships, and rapidly changing technology have all combined to drive managers to seek a more comprehensive understanding of risk and its management [Rasmussen 2007]. Whereas in the past, risk was managed in isolated pockets by functions as IT security, internal audit, and legal, today there is growing recognition that these arenas intersect and affect each other. And IT risk is clearly involved in many types of business risk these days. Criminal activity, legal responsibilities, privacy, innovation, and operational productivity, to name just a few, all have IT risk implications. As a result, organizations need a new approach to risk, one that is more holistic in nature and that provides an integrative framework for understanding risk and making decisions associated with it. Accomplishing this is no simple task, so developing such a framework will likely be an ongoing activity, as experts in IT and others begin to grapple with how to approach such a complex and multi-dimensional activity. This paper has therefore not tried to present a definitive approach to risk management. There was general agreement in the focus group that organizations are not ready for this. Instead, we have tried to sketch an impression of how to approach risk management and what an effective risk management program might look like. IT managers and others are left to fill in the details and complete the portrait in their own organizations.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to world wide web pages. Readers who have the ability to access the web directly from their word processor or are reading the paper on the web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Austin, R., and C. Darby (2003). The myth of secure computing, *Harvard Business Review* (Vol. 81) No. 6, pp. 120–125.

Baccarini, D., G. Salm, and P. Love. (2004) Management of risks in information technology projects, *Industrial Management + Data Systems* (Vol. 104) No. 3–4, pp. 286–293.

Berinato, S. (2007). The fifth annual global state of information security, *CIO Magazine* (28 August) www.cio.com.

Caldwell, F., and R. Mogull (2006). Risk management and business performance are compatible, Gartner Research #G00140802 (18 October).

Coles, R., and R. Moulton (2003). Operationalizing IT risk management, *Computers and Security* (Vol. 22) No. 6, pp. 487–493.

Day, G. (2007). Is it real? Can we win? Is it worth doing?: managing risk and reward in an innovation portfolio, *Harvard Business Review* (Vol. 85) No. 12, pp. 110–121.

Hillson, D. Danger ahead, *PM Network* **(**March 2008), www.pmi.org.

Hunter, R., G. Westerman, and D. Aron. IT risk management: a little bit more is a whole lot better, Gartner Exp CIO Signature Report (February 2005).

Hunter, R., and G. Westerman (2007). *IT Risk: Turning Business Threats into Competitive Advantage*. Boston: Harvard Business School Press.

Jordan, E., and L. Silcock (2005). *Beating IT Risks*. Chichester, England: John Wiley and Sons.

McKeen, J., and H. Smith (2003). *Making IT Happen: Critical Issues in IT Management*. Chicester, England: John Wiley and Sons.

Mogull, R. Gartner's simple enterprise risk management framework, Gartner Research # G00125380 (10 December 2004).

Nolan, R., and W. McFarlan (2005). Information technology and the board of directors, *Harvard Business Review*, (Vol. 83) No. 10, pp. 96–105.

Proctor, P. IT risk management for the inexperienced: a CIO's travel guide to IT "Securistan," Presentation to Gartner Symposium ITxpo 2007 Emerging Trends (22–26 April 2007), San Francisco.

Proctor, P. Key issues for the risk and security roles, 2008, Gartner Research #G00155764 (27 March 2008).

Rasmussen, M. Identifying and selecting the right risk consultant, Forrester Research Teleconference (12 July 2007), www.forrester.com.

Slywotzky, A., and J. Drzik (2005). Countering the biggest risk of all, *Harvard Business Review* (Vol.83) No. 4, pp. 78–89.

Symantec. Symantec internet security threat report: trends for July–December 2006 (Vol. XI) March 2007, Symantec Corporation.

Society for Information Management, Executive IT security, Private presentation to the SIM Advanced Practices Council, May 2008.

Witty, R. Findings: IT disaster recovery can upsell business continuity management, Gartner Research #G00155402 (19 February 2008).

APPENDIX A. A SELECTION OF RISK CLASSIFICATION SCHEMES ILLUSTRATING A VARIETY OF APPROACHES TO RISK IN USE TODAY

McKeen and Smith, 2003

- Financial risk
- Technology risk
- Security
- Information and people
- Business process
- Management
- External
- Risk of success

Rasmussen, 2007

- Information security risk
- Policy and compliance
- Information asset management
- Business continuity and disaster recovery
- Incident and threat management
- Physical and environment
- Systems development and operations management

Baccarini, Salm and Love, 2004

- Commercial risk
- Economic circumstances
- Human behavior
- Political circumstances
- Technology and technical issues
- Management activities and controls
- Individual activities.

Jordan and Silcocks, (IT Risks)

- Project risk
- IT services
- Information assets
- IT service providers and vendors
- Applications
- Infrastructure
- Strategic
- Emergent

Information Security Certification Consortium, 2007

- Management practices
- Access controls
- Telecommunications and network security
- Cryptography
- Security architecture and models
- Operations
- Application and systems development
- Physical security
- Business continuity and disaster recovery
- Laws, investigations and ethics

Combined Focus Group Categories, 2008

- Project
- Operations
- Strategic
- Enterprise
- Disaster recovery
- Information
- External
- Reputation
- Competitive
- Compliance & regulatory
- Forensic
- Opportunity
- Ethical
- Physical
- Business continuity
- Business process

ABOUT THE AUTHORS

Heather A. Smith (hsmith@business.queensu.ca) has been named North America's most published researcher on IT and knowledge management issues. A senior research associate with Queen's University School of Business at Kingston, Canada, she is the co-author of four books: *IT Strategy in Action; Management Challenges in IS: Successful Strategies and Appropriate Action; Making IT Happen: Critical Issues in IT Management;* and *Information Technology and Organizational Transformation: Solving the Management Puzzle.* A former senior IT manager, she is currently co-director of the IT Management Forum and the CIO Brief, which facilitate inter-organizational learning among senior IT executives. She is also a senior research associate with the Society for Information Management's Advanced Practices Council. In addition, she consults, presents, and collaborates with organizations worldwide, including British Petroleum, TD Bank, Canada Post, Ecole des Hautes Etudes Commerciales, the OPP, and Boston University. Her research is published in a variety of journals and books *including MIT Sloan Management Review, Communications of the Association of Information Systems, Knowledge Management Research and Practice, Journal of Information Systems and Technology, Journal of Information Technology Management, Information and Management, Database, CIO Canada,* and the *CIO Governments Review.* She is also a member of the editorial board of MISQ-E.

James D. McKeen is a professor of IT Strategy and Distinguished Research Fellow in MIS at the School of Business, Queen's University at Kingston, Canada. Jim received his Ph.D. in Business Administration from the University of Minnesota. He has been working in the IT field for many years as a practitioner, researcher, and consultant and is a frequent speaker at business and academic conferences. Dr. McKeen co-facilitates the networking of senior executives in the IT sector through two well-known industry forums: the IT Management Forum and the CIO Brief. He also has extensive international experience, having taught at universities in the U.K., France, Germany, and the U.S. His research has been widely published in various journals including the *MIS Quarterly*, *Knowledge Management Research and Practice*, the *Journal of Information Technology Management*, the *Communications of the Association of Information Systems*, *MIS Quarterly Executive*, the *Journal of Systems and Software*, *the International Journal of Management Reviews, Information and Management*, *Communications of the ACM*, *Computers and Education*, *OMEGA*, *Canadian Journal of Administrative Sciences, Journal of MIS*, *KM Review*, *Journal of Information Science and Technology* and *Database*. Jim is a co-author of three books on IT management with Heather Smith, the most recent being *IT Strategy in Action* (Pearson Prentice Hall, 2008). He currently serves on a number of editorial boards.

Copyright © 2009 by the Association for Information Systems. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712, Attn: Reprints; or via e-mail from ais@aisnet.org.

Communications of the Association for Information Systems

ISSN: 1529-3181

EDITOR-IN-CHIEF
Ilze Zigurs
University of Nebraska at Omaha

AIS SENIOR EDITORIAL BOARD

Guy Fitzgerald Vice President Publications Brunel University	Ilze Zigurs Editor, *CAIS* University of Nebraska at Omaha	Kalle Lyytinen Editor, *JAIS* Case Western Reserve University
Edward A. Stohr Editor-at-Large Stevens Institute of Technology	Blake Ives Editor, Electronic Publications University of Houston	Paul Gray Founding Editor, *CAIS* Claremont Graduate University

CAIS ADVISORY BOARD

Gordon Davis University of Minnesota	Ken Kraemer University of California at Irvine	M. Lynne Markus Bentley College	Richard Mason Southern Methodist University
Jay Nunamaker University of Arizona	Henk Sol University of Groningen	Ralph Sprague University of Hawaii	Hugh J. Watson University of Georgia

CAIS SENIOR EDITORS

Steve Alter University of San Francisco	Jane Fedorowicz Bentley College	Jerry Luftman Stevens Institute of Technology

CAIS EDITORIAL BOARD

Michel Avital University of Amsterdam	Dinesh Batra Florida International University	Indranil Bose University of Hong Kong	Ashley Bush Florida State University
Fred Davis University of Arkansas, Fayetteville	Evan Duggan University of the West Indies	Ali Farhoomand University of Hong Kong	Sy Goodman Georgia Institute of Technology
Mary Granger George Washington University	Ake Gronlund University of Umea	Douglas Havelka Miami University	K.D. Joshi Washington State University
Michel Kalika University of Paris Dauphine	Julie Kendall Rutgers University	Nancy Lankton Michigan State University	Claudia Loebbecke University of Cologne
Paul Benjamin Lowry Brigham Young University	Sal March Vanderbilt University	Don McCubbrey University of Denver	Fred Niederman St. Louis University
Shan Ling Pan National University of Singapore	Jackie Rees Purdue University	Thompson Teo National University of Singapore	Craig Tyran Western Washington University
Chelley Vician Michigan Technological University	Rolf Wigand University of Arkansas, Little Rock	Vance Wilson University of Toledo	Peter Wolcott University of Nebraska at Omaha
Yajiong Xue East Carolina University			

DEPARTMENTS

Global Diffusion of the Internet Editors: Peter Wolcott and Sy Goodman	Information Technology and Systems Editors: Sal March and Dinesh Batra
Papers in French Editor: Michel Kalika	Information Systems and Healthcare Editor: Vance Wilson

ADMINISTRATIVE PERSONNEL

James P. Tinsley AIS Executive Director	Vipin Arora CAIS Managing Editor University of Nebraska at Omaha	Copyediting by Carlisle Publishing Services