Communications of the Association for Information Systems

Volume 7 Article 13

9-8-2001

New Developments in Practice I: Risk Management in Information Systems: Problems and Potential

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

James D. McKeen
Queen's School of Business, Queen's University, jmckeen@business.queensu.ca

Sandy Staples
Queen's University, sstaples@business.queensu.ca

Communications of the Association for Information Systems

Volume 7, Article 13
August 2001

RISK MANAGEMENT IN INFORMATION SYSTEMS: PROBLEMS AND POTENTIAL

Heather A. Smith
James D. McKeen
D. Sandy Staples
Queen's School of Business
Queen's University
hsmith@business.queensu.ca

TUTORIAL;
RESEARCH

RISK MANAGEMENT IN INFORMATION SYSTEMS: PROBLEMS AND POTENTIAL

Heather A. Smith
James D. McKeen
D. Sandy Staples

Queen's School of Business
Queen's University

hsmith@business.queensu.ca

ABSTRACT

Risk management can be an extremely powerful approach to dealing with the complexities and uncertainties that increasingly surround technological change and its management. Conventionally in information technology (IT) projects, risks have been narrowly defined. Today, with IT becoming integral to a company's existence, the stakes are considerably higher and broader in scope. However, risk is sometimes seen a negative concept in information systems (IS) organizations because it implies that something could go wrong with an IT project. To understand effective risk management in IS, the authors convened a focus group of senior IS managers from a number of organizations in a variety of industries. The results of this discussion, the managers' presentations, and a review of the current research on risk management, were integrated and are presented in this paper. The nature of risk, identifying risk in IT initiatives, determining appropriate levels of risk, and dealing with unacceptable types and levels of risk are discussed.

The following conclusions were reached. Risk management is a means to an end – whether it is a successful IS project; stable, secure technical

operations; or a properly implemented business strategy using technology. It is not a one-time activity, but rather an ongoing process of identification, assessment, and action, which needs to be well integrated into every part of IS management. IS managers must learn to control both the problems and the potential that risk represents. Several general principles to help IS managers deal effectively with risks were identified. Effective risk management involves taking a holistic approach to risk, developing a risk management policy, establishing clear accountabilities and responsibilities, balancing risk exposure against controls, being open about risks to reduce conflict and information hiding, enforcing risk management practices, and learning what works and doesn't from past experience.

Keywords: risk management, risk assessment, information systems, project risk

I. INTRODUCTION

'Risk' can be perceived to be a negative word in IS organizations because it implies that something could go wrong with an IT project. This negative perspective conflicts with many IS professionals' traditionally optimistic worldview and with a management philosophy that makes it seem harsh and disloyal to talk about a plan's down sides. Where risk is addressed in IS, it is commonly used only as a factor to modify a system's potential financial returns, rather than as a management practice [KPMG Study, 1999]. Thus to date, risk assessment and management is something that is done minimally if at all in IS. For example, studies show that only one-third of senior executives feel that they understand IS risks well [Wah, 1998]. Even those companies that use formal risk management processes for other parts of their business demonstrate consistently poor IS risk management and take a fragmented approach to it [Hoffman, 1998]. Typically, organizations do not make IS risk management a priority, don't link IS risks to business strategy, and don't put enough effort into anticipating problems [Wah, 1998]. Therefore, the practice of IS risk management in organizations varies greatly [KPMG Study, 1999].

Risk management can be an extremely powerful approach to dealing with the complexities and uncertainties that increasingly surround technological change and its management. Conventionally in IS projects, risks are defined narrowly, e.g., would a project meet all its objectives or would it be implemented on time? Today, with IS becoming integral to a company's existence, the stakes are considerably higher and broader in scope. As systems become more interconnected, the things that can go wrong increase significantly. Furthermore, with companies adding new partners, untried technologies, and challenging business strategies to the mix, senior executives are beginning to realize that serious human and organizational risks are associated with the use of IS. Finally, with rapidly changing business and technology environments, some companies are required to take bigger and bigger risks to remain competitive. Therefore, effective risk management is now a much more important issue to both IS and business managers.

To learn more about risk management in practice today, a focus group was held in Toronto, Canada with senior IS managers from a wide range of industries. The results from this discussion and a review of the current research on risk management were integrated and are presented in this paper. Our objective is to provide a state-of-the-art summary on managing risk in information systems projects.

The paper is organized as follows. Section II describes the focus group methodology. Section III examines the nature of risk and provides an overview of the risk management process. The following three sections then explore the three steps of this process in more detail. They look at identifying risk in IT initiatives, determining appropriate levels of risk, and dealing with unacceptable types and levels of risk. Section VII presents conclusions.

II. RESEARCH METHODOLOGY

A focus group was held with 17 senior IS managers – most of whom report directly to the CIO – from various organizations including:

- 4 financial institutions
- 3 retail organizations
- 3 high-technology manufacturing organizations, and
- 3 telecommunications companies and
- 4 insurance companies

The majority of attendees held VP level positions, spearheading functions such as “business development”, “architecture”, “strategic planning”, and “integration services”.

FOCUS GROUPS

Judd et al. [1991] suggest that focus groups are a relatively cost-effective technique since they bring many people together at once to provide data on highly specific topics. Krueger [1989] offers more specifics on the purpose and logistics of a typical focus group.

> .... a focus group can be defined as a carefully planned discussion designed to obtain perceptions on a defined area of interest in a permissive, non-threatening environment. It is conducted with approximately seven to ten people by a skilled interviewer. The discussion is relaxed, comfortable and often enjoyable for participants as they share their ideas and perceptions. Group members influence each other by responding to ideas and comments in the discussion [p. 18].

> Focus groups produce qualitative data that provide insights into the attitudes, perceptions, and opinions of participants. These results are solicited through open-ended questions where respondents are able to choose the manner in which they respond and also from observations of those respondents in group discussion. The focus group presents a natural environment where participants are influencing and influenced by others – just as they do in real life. The researcher serves several functions in the focus group: moderating, listening, observing, and eventually analyzing using an inductive process. The inductive researcher derives understanding based on the discussion as opposed to testing or confirming a preconceived hypothesis or theory [p. 30].

QUESTIONS CONSIDERED

To guide and stimulate the thinking of the participants of the focus group, prior to the meeting participants were given a series of questions outlining potential issues involved in risk management. These questions were:

1. What is your working definition of risk?
2. How important is risk management in your organization today and why?
3. How do you identify and assess risk in your IS organization?
4. Do you use a formal risk management methodology? If so, how does it work? When do you use it?
5. What effective or ineffective risk management practices have you implemented?
6. Do you address risk management issues with users? Why or why not?
7. What are the risks of not doing risk management and/or the benefits of doing risk management?
8. Do you agree that risk assessment should be a primary management tool in IS?

THE MEETING

Each of the questions was discussed during the focus group meeting, which lasted 6.5 hours. The participants shared their views and the practices of their organizations. Two of the authors were present to moderate the discussion and capture the key points on flipcharts and by taking notes. They also collected presentations that the participants prepared in advance.

III. WHAT IS RISK AND HOW IS IT MANAGED?

IS managers and researchers traditionally define risk only in terms of negative consequences. For example, Aubert et al. [1998] use Boehm's definition: *"the possibility of loss or injury".* Focus group members described it similarly as *"the possibility of loss or damage"* and *"the possibility of suffering harm or loss".* Although this view of risk is widely used, Billington [1997] points out that, when examined closely, 'risk' can actually lead to both positive *and/or* negative

consequences. In any particular initiative, he notes, the risks involved could represent different meaning to an organization. There are three dimensions of a risk:

1. A *hazard* that must be minimized or eliminated.
2. An *uncertainty* about which path should be taken and which must be studied to reduce the variance between anticipated outcomes and actual results.
3. An *opportunity* for growth or improvement, which must be assessed to determine *how much* innovation, initiative, and entrepreneurship, should be exercised.

Viewing risk as something more than a hazard is highly applicable to risk management in IS. Although IS risks *can* lead to negative results, they can also represent significant opportunities for savings or business development. Because technology and its applications change rapidly, the vast uncertainty surrounding information technology is one of the biggest challenges an IS manager faces. Thus, this paper explores IS risk and its management in all its dimensions, recognizing that not all risk leads to negative consequences and not all risk needs to be eliminated.

LEVELS OF RISK

Several members of the focus group saw IS risk as operating largely at the level of IS projects. They defined it as: "the cumulative effect of the changes of uncertain occurrences which may adversely affect project objectives" and "the potential event or occurrence that may jeopardize the success of a project or cause it not to achieve one or more of its objectives." However, the discussion also made it plain that companies now perceive IS risk can exist at two other, broader levels.

1. IS can have an impact on a company's operations. The consequences of technology failure or declining service, and how systems work with business processes, can affect both a company's internal and external effectiveness and/or efficiency.

2. A firm's use of technology is often central to its overall business strategy. IT can influence a company's reputation and relationships, as well as its competitiveness and profits.

Because risk works in three dimensions (hazard, uncertainty, opportunity) simultaneously, it has qualities that cut across all of them. For example, the uncertainty involved in a project or an operating environment can affect business performance just as an uncertain business climate can affect a project's success.

RISK MANAGEMENT

The different dimensions (hazard, uncertainty, opportunity) and levels (project, operational, and strategic) of risk each need to be properly understood and managed. Carnegie Mellon's Software Engineering Institute website (www.sei.cmu.edu) explains that without risk management, companies are continually 'fire-fighting'. With a risk management program in place, companies shift to proactive decision-making that tries to anticipate and avoid problems before they occur. It notes:

> *"A successful risk management practice is one in which risks are continuously identified and analysed for relative importance. Risks are mitigated, tracked and controlled to effectively use resources."*

Risk management can provide managers with insights into what *could* happen. Consequently, without risk management more effort is spent correcting problems that could have been avoided sooner, success and failure can occur without warning, and decisions are made without complete information or adequate knowledge of future consequences.

Risk management involves three steps: identification, assessment, and dealing with the risk.

1. The first step is to identify the risks involved in a particular initiative to determine what could go wrong. Often risk management stops at this step, which accounts for the overwhelmingly negative impression associated with risk. Typically, risks are defined narrowly in terms of schedule,

budget, and technology. While these factors are important, as Section IV makes clear, risk comes in many sizes and shapes. Identifying *all* of the risks involved – especially digging out the ones that are masked by assumptions or hidden by imperfect knowledge – is therefore an essential first step to determining how to manage them.

2. The second step is to assess the company's exposure to the risks identified. Assessment includes determining both the likelihood of the risk occurring and the potential impact if it occurs. Not all risks will occur and not all risks will have a significant effect on an initiative or a strategy. Thus, risk exposure is a function of how these two aspects work together. While risk assessment tends to focus on the consequences of a failure (i.e., what will be lost?), our focus group members also pointed out that corporate impacts could be generated by extreme success as well as failure (e.g., too much demand on a system).
3. Dealing with risk is the third step. Effectively addressing risk involves using a continuum of strategies that depend on the nature and amount of risk involved. In some cases, simply monitoring the risk is adequate, in others, action should be taken to mitigate or reduce risk. Sometimes, anticipation of risk can lead to plans to deflect impacts (as with insurance) or contingency planning may be necessary if rapid recovery is essential [Aubert, 1998].

In short, risk management is a forward-looking activity that makes the potential problems, opportunities, uncertainties, and threats implicit in an initiative explicit to management. It is a formal process by which risk can be brought under control and whereby surprises are minimized. The next three sections of this paper explore these three steps of risk management in more detail.

IV. IDENTIFYING RISK

To assess the risks involved in an initiative, it is essential to understand where they originate. Risk arises from many different general sources. In this

section, we explore these sources of risk and illustrate how one source of risk can have one or more dimensions (i.e., it can represent a hazard, uncertainty or opportunity) and operate simultaneously at the project, operations and business strategy level in an organization.

FINANCIAL RISK

It has long been understood that the financial return of an IS project should be greater than the amount invested in it. For this reason, return on investment (ROI) is usually computed for IS projects. Dué [1996] notes that typically, an IS investment's estimated return needs to be adjusted by between 10% and 25% to account for the chance that it will not pay off as expected. The risk of overestimating benefits and underestimating costs is a real one, as many companies can attest. However, a straightforward cost-benefit analysis is only appropriate for situations where the value of IS derives primarily from operational efficiencies.

Venkatramen [1997] points out that although companies historically managed most IS activities on the basis of rigid, quantitative payback criteria, they can be vulnerable financially from sources not quantifiable using ROI. For example, at a *business strategy* level, companies may need to invest simply to keep opportunities open or to support new organizational strategies [Luehrman, 1998; Venkatramen, 1997]. *Operationally,* investment may be needed to support current business capabilities or create new ones. Furthermore, even at a project level, the risks of being over budget or behind schedule must be balanced with the longer-term cost of errors if a system is installed too rapidly. Thus, while ROI continues to be an important element of financial risk, it should not be the only financial factor considered in risk assessment.

TECHNOLOGY RISK

New and untried technology increases the risk of project failure because neither IS professionals nor users understand it well [McFarlan, 1981]. Technology performance, scalability, reliability, and stability are other sources of risk that can impact a project's success. However, organizations are now

recognizing that technology can represent a risk at other levels as well. Several focus group members pointed out that their companies consider technology to be both an operating risk (i.e., that general technology failures could prevent business from being conducted) and a strategic risk (i.e., that outdated technology will result in a loss of market share and render the company non-competitive).

Operationally, with more and more business functions being automated, an effective technology infrastructure (i.e., hardware, software, networks, and processes) – or the lack of one -- is now a significant factor in how a company conducts its business [Wah, 1998]. Champey [1998] points out that operational failure of technology brought new meaning to the term “killer application” at some companies. *Strategically*, there is not only the risk of choosing the wrong technology but also of implementing it poorly and thereby awakening the competitive instinct of other organizations, raising the cost of doing business [Prakash, 1998], or losing new business opportunities.

SECURITY RISK

Security is the ability for a business and its customers to trust the electronic environment in which the company operates and offers its services [Garigue & Mackie, 1999]. In the past, security risk most often referred to the hazards represented by unauthorized system access or by general disasters. Today, application security (including user authentication, control and authorization) and data integrity continue to be risks at a *project* level. However, with the increasing electronic interaction between companies and with individuals, network defensibility (local, wide area, and global) is a major *operating* hazard. Network, system, and file protection are all general security risks that must be addressed at an organization level, and even beyond. Thus, security management and security awareness also contribute to the levels of operating risk a business faces. Companies must assess whether passive protection mechanisms (e.g., virus scanning, encryption, and firewalls) are adequate for their needs or whether more active protection, such as vulnerability analysis and intrusion detection, is needed.

INFORMATION RISK

Commonly, information risk is perceived to arise from data that is inaccurate or missing in a system. However, there is growing recognition that information risk is broader, cutting across all levels of organization management and control. Newer information risks include privacy, decision-making and strategy development risks. Privacy became a more important hazard with the advent of privacy legislation in many jurisdictions that regulates what information can be collected about individuals and how it can be used [Smith and McKeen, 1999]. Peladeau [1995] points out that the most common sources of information risk are collecting too much information and not disposing of unneeded or outdated material.

A second source of risk is that information can be used to make improper decisions about business situations (i.e. decision-making risk). Information embedded in systems and in organization controls as assumptions or internal logic is often not apparent to decision-makers. This type of information, if improperly understood or represented, can produce an illusion of control for managers while affecting many aspects of business operations such as model assumptions, human resources, accounting, liquidity, credit, legal and other operating processes [Marshall et al., 1996].

Since information is the means by which managers deal with uncertainty and complexity, they face the risk that they will not have the information they need, in the right format, and at the right time, to make strategic decisions [Marshall et al., 1996].

PEOPLE RISK

While it is often easy to see technological risks, people must be factored in to risk management just as much [Wah, 1998]. People are a source of uncertainty because of the variety of ways they can react to information technology and its challenges. Because people respond subjectively to change, their reactions can be difficult to predict. Thus, users at all levels can respond either positively or negatively to a new system, as can external customers. Both

can create risk for a company, especially if the reaction is extreme and unanticipated.

Focus group participants pointed to other sources of people risk in a *project* which are sometimes ignored, including

- inadequate project resource management,
- poor decision-making competency at all levels,
- poor expectations management,
- lack of relationship building with everyone involved in an initiative, and
- failure to match the pace of change to a staff's ability to cope with it.

Pressure, burnout, and loss of face are other risks that are sometimes not apparent in a company's haste to implement new information technology projects.

At the *operational* and *strategic* levels, people risk may be less obvious, but is equally uncertain. The influence of corporate power politics cannot be ignored in business decision-making around information technology as many IS managers found out to their dismay. For example, one focus group member noted that conflict is a major reason why risk is not adequately addressed in organizations at senior levels.

BUSINESS PROCESS RISK

Information systems are frequently used to make changes in business processes to reduce operating costs. The greater the change being made, the greater the risk involved. Major transformations in a number of business areas typically require the large-scale transformation of jobs, competencies, procedures, workflow, management, and decision-making. If successful, these changes can make an organization more effective and/or more efficient. However, if not properly managed, they can represent a threat to organizational survival [Yetton et al., 1994].

Often, the impact of a change (and hence, the type of risk involved) is not clearly visible to senior management. Simons [1999] explains that people at the top of an organization are usually less aware of business process risk than those

lower down. He notes that when processes change, information flows change and this often creates operational havoc. Internal reporting systems measuring critical performance variables can be affected as well. Focus group members also cited lack of technology usability, poor help desk and support problems, inadequate training, and unanticipated results, as contributing to business process risk.

MANAGEMENT RISK.

Every project involves its own special set of vulnerabilities and dependencies which need to be managed, e.g., schedule, budget, functionality, compatibility, relationships, expectations, and communication. The quality of the management brought to bear on these issues (including how they are planned for, identified, assessed, dealt with, and balanced against one another), will do a great deal to enhance or detract from the success of a project [Dieckmann, 1996]. Similarly, the quality of IS management as a whole will contribute strongly to the hazards, uncertainties, and opportunities facing an organization's operations and business strategies. For example, if a company has weak IS capabilities, particularly if it is in a competitive industry, management of the IS assets can become a corporate liability.

EXTERNAL RISK

Risk from external sources received considerably more attention with the growth of IS outsourcing, IT subcontracting, ERP systems, and other forms of pre-packaged software [Champey, 1998; Aubert et al., 1998]. Companies can find it very tempting to buy a 'shrink-wrapped' solution off the shelf. Focus group members pointed out that external projects need to be assessed and managed for risk just like any other system development project, since they face many of the same schedule, budget, and implementation problems. In addition, risk can come from:

- making too many customized changes
- assumptions embedded in the software
- poor contract management
- limited understanding of the business requirements to be addressed
- the stability of the software development company
- The software development company's responsiveness to the unique needs of the purchasing company.

As the size of the software package increases, risk increases in all areas. Enterprise Resource Planning (ERP) systems affect many business divisions and business processes are more risky than single-purpose applications.

When a company decides to outsource some or all of its IS functions, overall business risk can also increase. Aubert et al. [1998] identified three key risk factors in outsourcing:

1. Client capacity, including lack of experience and expertise with contracts and contract management,
2. Supplier capacity, including supplier stability, size, and expertise, and
3. The nature of the outsourcing activities, including their interdependence with internal activities, their proximity to core competencies, the availability of competitors, and clarity of success factors and measures.

With outsourcing, companies are not only vulnerable to increased costs but also to such factors as increased rigidity, poor support and technological lock-in. Each of these risks can seriously impact both an organization's ability to operate effectively and/or efficiently and its implementation of business strategy.

RISK OF SUCCESS

A frequently neglected source of risk, but one that can have equally devastating consequences for a company, is the risk of success. Focus group members explained that projects can be as unprepared for success as they are for failure. Success can mean a higher volume of transactions than expected or that users see more potential in an application than was originally anticipated. Both can lead to demand for expansion of a project. Thus, scalability of volume

and function are two key risks of success at a *project* level. Simons (1999) explains that success can increase the level of *operational* risk because rapid expansion can mean that the resources, processes, and structures of a company are inadequate to the change. Performance measures, controls, and jobs may all need to be redefined as a result.

Risk identification is fundamental to risk management. If managers do not know where risk exists in an organization, they cannot act. Almost all the focus group members reinforced this point as being a significant limiting factor in their ability to manage risk effectively. Unfortunately, they stated, the biggest problems arise not from being unable to identify risk, but from being unable to incorporate it into their project, operations and strategic plans.

V. ASSESSING RISK

Risk is endemic and cannot be eliminated altogether. The challenge for IS managers is to determine how much risk they are facing with an initiative and to assess whether or not this level of risk is appropriate for their business. Evaluating risk exposure is an art, not a science. Most assessment methods involve assigning a probability of occurrence and evaluating each individual risk factor on scales of impact (e.g., 1 = no impact, 3 = high impact; or 1 = very unlikely to occur and 7 extremely likely to occur). These risks can be documented using such tools as a checklist (Table 1) or a graph (Figure 1). In Table 1, multiplying impact by probability yields an overall risk exposure value that can be compared to a pre-determined degree of acceptable risk.

Since risk exposure is a subjective measure, what is more important than the assessment method used is ensuring that everyone involved in an information technology venture – at all levels – agrees on the level of risk involved and can accept it. It seems that developing common understanding about risk is at least as important in managing it as the actual levels of risk involved. McFarlan [1981] writes:

Table1. Sample Risk Evaluation Checklist for External Dependencies

Risk Factor	Likelihood of Occurrence	Potential Impact
Risk #1		
Risk #2		
Risk #3		
Risk #4		
Risk #5.....		

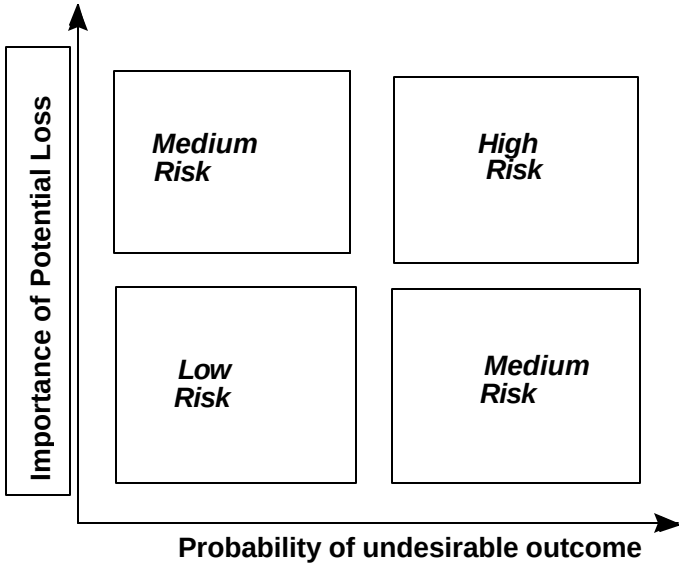

Figure 1. Possible Levels of Risk
[after Aubert et. al., 1998]

"Often fiascoes occur when senior mangers believe a project has low risk and IS managers know it has high risk. In such cases, IS managers may not admit their assessment because they fear that the senior executives will not tolerate this kind of uncertainty ... and will cancel a project of potential benefit to the organization."

Others believe that it is IS that is always searching to eliminate risk and that business is more comfortable with higher levels of risk exposure [Maccoby, 1997; Knowles, 1996]. Focus group participants saw misalignment of how risk is viewed as a major inhibitor of effective risk management, as the following comments demonstrate:

> *"Management blocks out risk messages. It's not safe to send them; it's better to say everything's okay."*
> *"If you take a risk and fail*, *you could lose your job."*
> *"If you identify a risk, you'd better have a solution"*.

Acceptable levels of risk need to be monitored continuously. The key to risk assessment is not to identify an arbitrary risk exposure number that is "too high" but to ensure that there is agreement about how much risk is involved and then to work to make sure that the levels of risk involved are appropriate for the business. One of the best ways to do so is to 'package' risk into some sort of graphical format so that everyone can clearly view and understand the risk involved in key areas. Some organizations in the focus group categorize risk exposure by the major sources of risk (e.g., technical, external etc.) and color-code them green, yellow, and red for the levels of risk involved. These colors can then be linked in a table or in a web-diagram that show all types and levels of risk together.

VI. DEALING WITH RISK

Once risks have been identified and an appropriate level of exposure agreed on, the final step in risk management is to determine what to do about each risk. Again, there is a great deal of variation in specific risk management strategies by company. From the focus group participants, the authors collected over 50 practices being used by IS managers. These practices are listed in the Appendix. When these practices were analyzed, a number of more general principles for dealing effectively with all types of risk emerged. These principles

would be advisable for any organization to implement, regardless of industry or degree of risk tolerance, and are presented below.

TAKE A HOLISTIC APPROACH TO RISK

Risk management cannot be effective unless it is understood in all its dimensions and seen as intrinsic to projects, operations, and business strategies. Risk management is a cycle that must be repeated continually. Focus group members were clear that risk management is an ongoing process that requires continual follow-up. New hazards, uncertainties, and opportunities regularly appear on the horizon even as others are managed effectively. Risk assessments too, will change as more knowledge becomes available, technologies improve, and the business environment changes.

DEVELOP A RISK MANAGEMENT POLICY

Companies should develop a framework to establish the standards and protocols needed to manage risk in their particular business. Such a policy:

- integrates IS risk management with the general strategies and policies of managing the business
- makes risk both visible and acceptable to talk about.
- develops a common understanding of what is an appropriate level of risk.
- ensures consistency in risk assessment.
- identifies specific mechanisms to manage IS risk within the organization.

To establish a policy, a firm can create a technology policy committee, enhance the role of the internal audit group, or develop templates which ensure that IS work as a whole can be properly monitored by senior management.

ESTABLISH CLEAR ACCOUNTABILITIES AND RESPONSIBILITIES.

Once risks are identified, it is extremely important to assign responsibility for managing and monitoring individual risks. At a project level, the project manager is an obvious candidate for overall responsibility. Many of the focus group participants' organizations also assign more general risk management functions to an audit team, an architecture review team, or a quality assurance

group. Focus group participants pointed out that because these external groups tend to be knowledgeable in specific areas of risk management, they can be extremely helpful in managing risk if they are involved early in the project's development

BALANCE RISK AND CONTROLS

It is easy to slip into a risk averse mentality with IT projects because so much is uncertain and so much can go wrong [Knowles, 1996]. It is also possible that, given the typical technical and scientific backgrounds, IS professionals may generally tend to be risk-averse. But managing risk into the ground is a guaranteed way to kill innovation [Maccoby, 1997]. Many risks in IS initiatives only need to be monitored, not controlled [Aubert et al., 1998]. While controls are essential in the case of some risks, the use of formal controls should always be balanced against the level of risk exposure involved.

BE OPEN AND REDUCE CONFLICT

Focus group participants agreed that one of the surest ways to inhibit risk management is to enter into a negative spiral of conflict and fear. Once this happens, trust is destroyed and damage escalates [Maccoby, 1997]. A key risk management principle is therefore to create an environment of openness. While trust cannot be decreed, it can be built by management through, for example, strategic leadership, good coaching, and treating people with respect [Maccoby, 1997]. A positive attitude towards risk management not only takes pressure off staff, it enables them to share hard news with senior management when necessary.

ENFORCE RISK MANAGEMENT DISCIPLINES

As companies begin to pay more attention to risk, it will become clear which practices are most helpful in managing risk at the project, operations, and strategic levels. These practices need to be adopted as disciplines within the overall risk management framework. Disciplines such as architectural reviews, reviews with a project management office, budget and schedule controls, and audit controls, need to be enforced consistently and rigorously. Properly

designed, they can serve as an early warning system to senior management, address commonly understood risks that may arise due to inexperience or inattention, and help reduce uncertainty at all levels.

LEARN WHAT WORKS AND WHAT DOESN'T

Finally, extracting lessons learned in risk management can enhance an organization's effectiveness. Learning how to identify and document lessons learned in a way that is relevant to others, repeatable, and accessible when needed, is not easily done. However, implementing learning disciplines will have a considerable impact on reducing risk at both a project and operations level.

VII. CONCLUSION

Risk management is a way of thinking that continually seeks to ensure that the risk-to-reward ratio is in balance for a company. In this paper, we examined risk management as a means to an end – whether it is a successful IS project, stable, secure technical operations, or a properly implemented business strategy using technology. It is not a one-time activity, but rather an ongoing process of identification, assessment, and action, which needs to be well integrated into every part of IS management. The pace of change in information technology and business implies that risk cannot be ignored or dealt with only when it arises. IS organizations cannot afford to deal with it through fire fighting. Instead, IS managers must learn to control both the problems and the potential that risk represents.

Editor's Note: This article was received on July15, 2001 and was published on September 8, 2001.

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.

Aubert, B., M. Patry, and Rivard, S. (1998). "Assessing the Risk of IT Outsourcing," *Proceedings of the 31st Hawaii International Conference on Systems Sciences*. California: IEEE, 685 – 693.

Billington, J. (1997). "A Few Things Every Manager Ought to Know About Risk," *Harvard Management Update*, 2(3), March, 1 – 12.

Champey, J. (1998). "Killer Technologies," *Forbes*, 162(5), September 7, 180 – 181.

Dieckmann, M. (1996). "Making New Technology Investments Pay Off," *Managing Office Technology*, 41(7), July, 14 – 26.

Due, R. (1996). "The Value of Information," *Information Systems Management*, 13(1), Winter, 68-72.

Garigue, R. and A. Mackie, (1999). "From Provincial Action to National Security: A National Information Protection Agenda for Securing Government in Cyberspace," Bromont, Quebec: *Third Lac Carling Conference on Electronic Service Delivery*, May.

Hoffman, T. (1998). "Risk Management Still a Wild Frontier," *Computerworld*, 32 (7), February 16, 10.

Judd, C. M., E. R. Smith, and L. H. Kidder, (1991). *Research Methods in Social Relations.* Toronto: Holt, Rinehart and Winston

Knowles, J. (1996). "Learn to Bungee Jump," *Datamation*, 42(16), October, 29.

KPMG Study (1999). *The Risk Survey Report*, Risk Strategy Services, Toronto: KPMG Consulting.

Krueger, R. A. (1989). *Focus Groups: A Practical Guide for Applied Research.* Newbury Park, CA: Sage Publications.

Luehrman, T. (1998). "Strategy as a Portfolio of Real Options," *Harvard Business Review*, 76(5), September-October, 89 - 101.

Maccoby, M. (1997). "Building Trust is an Art," *Research Technology Management*, 40 (5), September/October, 56 - 58.

Marshall, C., L. Prusak, and L. Shpilberg, (1996). "Financial Risk and the Need for Superior Knowledge Management," *California Management Review*, 38(3), Spring, 77 – 101.

McFarlan, W. (1981). "Portfolio Approach to Information Systems," *Harvard Business Review*, 59(5), Sept-Oct, 142-150.

McKeen, J., and H. Smith, (1997). "Developing Effective I/S Project Managers," *The I/T Management Forum* – Kingston, ONT: Queen's University School of Business, 7 (1), February.

Peladeau, P. (1995). "Principles of Personal Data Protection," *Risk Management*, 42(12), December, 35 – 40.

Prakash, A. (1998). "Leveraging the Potential of Strategic Systems," *Information Systems Management*, 15(1), Winter, 58-63.

Simons, R. (1999). "How Risky is your Company?" *Harvard Business Review*, 77 (3), May-June, 85-94.

Smith, H. and J. McKeen, (1999). "The CIO Brief on Privacy," *The I/T Management Forum* – Kingston, Ont: Queen's University School of Business.

Software Engineering Institute (SEI) (1999). SEI Risk Management Frequently Asked Questions,www.sei.cmu.edu, Carnegie Mellon University, (referenced April 14, 2001).

Venkatramen, N. (1997). "Beyond Outsourcing: Managing IT Resources as a Value Center," *Sloan Management Review*, 38(3), Spring, 51 - 64.

Wah, L. (1998). "The Risky Business of Managing IT Risks," *Management Review*, 87(5), May, 6.

Yetton, P, W. Johnston, and K. Craig, (1994). "Computer-aided Rrchitects: a Case Study of IT and Strategic Change," *Sloan Management Review*, 35(4), Summer, 57 - 68.

APPENDIX A

SELECTED RISK MANAGEMENT PRACTICES

This appendix lists 50 practices IS managers use to manage risk The list is based on input from focus group participants (Section VI).

PROJECT PRACTICES

Risk Identification

- brainstorm risk as a team
- work with clients to develop a 'what if' plan
- employ risk checklists and templates
- calculate return on investment
- do an anonymous survey of users and IS staff
- conduct a project post-mortem

Risk Assessment

- update risk assessments after every project phase
- undertake a formal impact assessment

Risk Mitigation/Control

- document and monitor the business case
- establish clear objectives and requirements
- spend time and money up front with vendors to clarify requirements
- document requirements in vendor contracts
- use a project methodology
- hold project reviews
- enforce project planning
- ensure proper testing
- create a project support office
- develop worksheets for all documentation needed

- use estimating tools
- establish a SWAT team of experienced staff to help if the project gets stuck
- pay vendors by deliverables not time and materials
- create a support and maintenance plan for packaged software
- get references for vendors and suppliers.
- create contingency plans for high risk items
- implement in small pieces
- increase project management competencies
- provide a mentor for inexperienced project managers
- develop a training strategy

OPERATIONS PRACTICES

Risk Identification

- research technology changes
- appoint a chief risk officer
- establish a lessons learned data base

Risk Mitigation/Control

- develop contingency plans for high risk situations
- create risk management plans for computer operations and data management
- implement architectural reviews of all technology initiatives
- hold security and technology reviews
- establish technical and quality assurance groups
- monitor defects
- investigate and implement estimating tools
- develop risk metrics
- establish access, security and privacy standards
- keep organizational changes relatively small

BUSINESS STRATEGY PRACTICES

Risk Identification

- monitor political, social and technology trends
- monitor the company's reputation, competition and regulation

Risk Mitigation/Control

- design the organization to deal with risk
- establish a clear business vision
- monitor business cases
- assign all IT initiatives a business executive sponsor
- once a vision has been agreed, move quickly
- take responsibility for risk
- integrate risk management into all business management activities.

ABOUT THE AUTHORS

Heather A. Smith, is Senior Research Associate in the School of Business at Queen's University, Kingston, Canada. A recognized authority on IT management, she is a former senior IT manager. For the past fifteen years she worked with North American organizations to identify and document leading-edge practices and to bring the best of academic research to practising IT managers. She is a founder and co-facilitator (with Jim McKeen) of the Queen's IT Management Forum, the CIO Brief, and the Knowledge Management Forum, which facilitate inter-organizational learning among senior executives, and co-author of *Management Challenges in IS: Successful Strategies and Appropriate Action.* She is a Research Associate with the Lac Carling Conference on E-Government and the American Society for Information Management and Chair of the IT Excellence Awards University Advisory Council. Her research has been published in the *Journal of Information Technology Management, Database, CIO Canada,* and the *Lac Carling Governments Review.* Currently, she is writing a book on virtual organizing, collaborating on an international research project to

discover new organizational models, and writing a book with Jim McKeen on IT strategy.

James D. McKeen, is Professor of MIS at the School of Business, Queen's University at Kingston, Canada and is the Founding Director of the Queen's Centre for Knowledge-Based Enterprises, a research think-tank for the knowledge economy. His research interests include IT strategy, user participation, the management of the IS function, and knowledge management in organizations. His research is published in the *MIS Quarterly*, the *Journal of Information Technology Management*, 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, JMIS*, and *Database*. He currently serves on the Editorial Board of the *Journal of End User Computing*, regularly reviews articles for many MIS journals, and was the MIS area editor for the *Canadian Journal of Administrative Sciences* for seven years.

Jim is a practitioner, researcher, and consultant. He and Heather Smith published a book based on their work with the IT Management Forum called *Management Challenges in IS: Successful Strategies and Appropriate Action* (Wiley UK, 1996) and are currently working on a book on IT Strategy.

Sandy Staples, Ph.D., is Assistant Professor in the School of Business at Queen's University, Kingston, Canada. His research interests include the enabling role of information systems for virtual work and knowledge management and assessing the effectiveness of information systems and IS practices. Sandy's articles appear in *Organization Science, Journal of Strategic Information Systems, Journal of Management Information Systems, Communications of the Association for Information Systems, International Journal of Management*

Reviews, Business Quarterly, Journal of End-User Computing, and *OMEGA*. He serves on the Editorial Advisory Board of the *Journal of End User Computing.*

Communications of the Association for Information Systems

ISSN: 1529-3181