Communications of the Association for Information Systems

Volume 14 Article 1

7-7-2004

A General, But Readily Adaptable Model of Information System Risk

Steven Alter
University of San Francisco, alter@usfca.edu

Susan A. Sherer
Lehigh University, sas6@lehigh.edu

Communications of the Association for Information Systems

A GENERAL, BUT READILY ADAPTABLE MODEL OF INFORMATION SYSTEM RISK

Steven Alter
School of Business and Management
University of San Francisco
alter@usfca.edu

Susan A. Sherer
College of Business and Economics
Lehigh University

ABSTRACT

This article is the first of two whose goal is to advance the discussion of IS risk by addressing limitations of the current IS risk literature. These limitations include:

- inconsistent or unclear definitions of risk,
- limited applicability of risk models,
- frequent omission of the temporal nature of risk, and
- lack of an easily communicated organizing framework for risk factors.

This article presents a general, but broadly adaptable model of system-related risk. The companion article, CAIS Volume 14, Article 2 [Sherer and Alter, 2004] focuses on IS risk factors and how these factors can be organized.

This article starts by identifying criteria for a general, but broadly applicable risk model. It compares alternative conceptualizations of risk and provides clarifications of the definitions of risk and of different treatments of goals, expectations, and baselines for assessing risk. It presents several of the risk models in the IS literature and discusses the temporal nature of risk.

Based on that background it presents a general and broadly adaptable model of risk that encompasses:

- goals and expectations,
- risk factors and other sources of uncertainty,
- the operation of the system or project whose risks are being managed,
- the risk management effort,
- the possible outcomes and their probabilities,
- impacts on other systems,

- and the resulting financial gains or losses.

The model's adaptability allows users to eliminate facets that are not important for their purposes. For example, the majority of current practitioners would probably think of risk in terms of negative outcomes rather than the full distribution of possible outcomes. A comparison of the general model with other risk models in the IS literature shows that it covers most of the ideas expressed by previous IS risk models while also providing a practical approach that managers can use for thinking about IS risk at whatever level of detail makes sense to them.

Keywords: information systems risk, risk factors, risk components, risk model, risk management, work system, project risk, software risk, work system framework, success factors, emergent risks

I. INTRODUCTION

This article is the first of two whose goal is to advance the discussion of IS risk. The article presents a general, but broadly adaptable model of system-related risk. The model applies both to information systems in operation and projects aimed at creating or improving information systems. The second article [Sherer and Alter, 2004] discusses the risk components and many risk factors in the IS literature. It shows how the risk factors can be organized to make them more accessible and more easily communicated to business managers.

This article starts by identifying criteria for a general, but broadly applicable risk model. It compares alternative conceptualizations of risk and provides clarifications related to definitions of risk, different treatments of goals, expectations, and baselines for assessing risk. It mentions several of the risk models in the IS literature and discusses the temporal nature of risk. Based on that background it presents a general and broadly adaptable model of risk that encompasses:

- Goals and expectations
- Risk factors and other sources of uncertainty
- Temporal relationships between goals, initial risk factors, emergent risk factors, and management goals and decisions
- Operation of the system or project whose risks are being managed
- Risk management and abatement activities
- Possible outcomes and their probabilities
- Impacts on other systems
- The resulting financial gains or losses.

The model's adaptability allows users to eliminate facets that are not important for their purposes. For example, the most general version of the model is based on the viewpoint of the decision science literature, and views risk as the probability distribution of outcomes, both positive and negative. An alternative, slightly less general model is presented that reflects the way most of the IS literature views risk in terms of negative outcomes relative to management goals and expectations. Omission of positive outcomes from the risk model is only one of many possible adaptations to meet different analysis needs of different users. A comparison of these two models with other risk models in the IS literature shows that these two models cover most of the ideas expressed by previous IS risk models while also providing a practical approach that managers can use for thinking about IS risk at whatever level of detail makes sense to them.

II. THE NEED FOR MORE CLARITY ABOUT INFORMATION SYSTEM RISK

Our attempt to develop a general, but readily adaptable model of information system risk was motivated by the results of a survey of the IS risk literature. Attempting to represent the

reasonably recent literature rather than covering the hundreds of articles directly or indirectly related to IS risk, our literature survey focused on three journals consistently ranked among the best IS research journals (*MISQ*, *ISR*, and *JMIS)* and selected articles starting in 1986 whose title included the word *risk* or whose abstract focused on risks in system projects or operation. We supplemented this group of articles with other risk-related articles that we believed were significant based on our knowledge of the literature. In total we included 46 articles. We believe these articles are a good representation of the literature. Appendix I categorizes these articles in terms of

- definition of risk,
- model or approach used,
- type of system or project (which reflects different stages of the software life cycle and some aspects of the temporal nature of risk), and
- number and type of risk variables.

The general conclusion from our literature survey is that the IS risk literature is a jumble of diverse risk models and partially overlapping, atheoretical lists of risk factors and risk components. This article addresses one shortcoming of the literature, the lack of a practical model that most managers can use for understanding IS-related risks at whatever level of detail is appropriate for them. Our companion article [Sherer and Alter, 2004] focuses on risk factors and delves further into the literature's coverage of risk components and risk factors.

To introduce ideas needed for a broadly adaptable risk model, this section provides clarifications related to conceptualizations of risk and different treatments of goals, expectations, and baselines for assessing risk. It refers to some of the risk models in the IS literature and discusses the temporal nature of risk.

Before discussing those ideas it is worthwhile to consider criteria that a general, yet broadly adaptable risk model should satisfy:

- Clarity: The model should be based on clearly defined concepts.
- Practicality of use: The model's use of concepts should be understandable to typical business professionals. It should provide rigor by organizing a risk analysis, but should not sacrifice practicality and efficiency for mathematical purity. In particular, it should not force users to provide data they find unintuitive or untrustworthy.
- Completeness: The model should encompass key issues that business and IT professionals care about. Omitting issues that users care about will make it less applicable to the situations in which it is needed.
- Adaptability: The model should be adaptable to the user's situation and interests. Users should feel free to include or exclude specific components of the model, but should be aware of both advantages and disadvantages of such omissions.

Our search of the existing IS risk literature found no risk models that we believe satisfy these four conditions. We found some models that address the needs of professional software developers, but none that we believe are truly practical for use by business professionals, complete in the issues that business professionals care about, and readily adaptable by users who may not be interested in all of the possible facets of a very general model.

CONCEPTUALIZATIONS OF RISK

The term risk has various meanings in everyday life. For example, definitions of risk provided by www.dictionary.com include:

- The possibility of suffering harm or loss; danger.
- A factor, thing, element, or course involving uncertain danger; a hazard

- For an insurer, the danger or probability of loss or the amount an insurance company stands to lose.
- In terms of variability: the variability of returns from an investment or the chance of nonpayment of a debt.
- A person or thing as a risk, such as a person considered a poor risk.

The IS risk literature uses several different conceptualizations of risk. Table 1 summarizes the distribution of risk conceptualizations in the 46 articles selected from the IS risk literature. Most of these conceptualizations focus on negative occurrences and fall into three categories: (1) risk components, (2) risk factors, and (3) probability of negative outcomes.

Table 1. Conceptualizations of Risk in 46 IS Risk Articles

Conceptualization of Risk	Number of articles
Risk components: different types of negative outcomes	11
Risk factors leading to loss or source of risk factors	11
Risk as probability of negative outcomes (sometimes weighted by loss)	15
Risk as difficulty in estimating outcome	2
Risk undefined or discussed using a different term such as problem or threat	7

Risk as Risk Components, Different Types of Negative Outcomes

The first conceptualization identifies different types of negative outcomes, such as project risk (failure to complete a project within budget, schedule and/or quality constraints), functionality risk (failure to deliver intended functionality), political risk (negative consequences of changing power relationships with users), or security risk (negative consequences of insecure systems). A limitation of this conceptualization is that these risk components can often overlap and therefore are not independent, contrary to what the term component typically means. For example, functionality risk can be viewed as part of project risk and sometimes can cause political risk and security risk.

Risk as Factors Leading to Loss

The second conceptualization of risk is as risk factors such as size of project, use of new software, or malicious employees. Some studies combine risk factors from various sources such as task, technology, or actors. Others subdivide these sources into finer categories, for example, specifying a type of actor such as customer or supplier. Our companion article identifies and organizes 228 risk factors found in the 46 articles in our literature search.

Risk as Probability of Negative Outcomes

Approximately one third of the studies suggest that risk should be measured as a probability distribution of negative outcomes, often weighted by financial loss. The probabilities of negative outcomes were subjective estimates or numbers computed based on statistical techniques.

CRITICAL CLARIFICATIONS

We believe that the IS risk literature emphasizes negative outcomes rather than the range of outcomes approach because it reflects managerial preoccupation with meeting goals. The emphasis on negative outcomes deserves further comment because the decision analysis literature typically uses a different definition. We will look at three related aspects of the definition of risk:

- Should IS risk focus on negative outcomes?
- What is the role of goals and expectations in IS risk?
- What is the baseline for assessing risk?

Should IS Risk Focus on Negative Outcomes?

In contrast to the emphasis on negative outcomes in the IS risk literature, decision analysts and operations researchers typically conceptualize risk as a probability distribution of possible outcomes based on a model that starts with probability distributions for important parameters. Those probability distributions may be discrete or continuous. For example, discrete probabilities often appear in decision tree examples related to whether or not to drill for oil based on parameters of the local geology, whereas continuous distributions may appear in examples related to complex R&D decisions in pharmaceuticals. In decision trees with discrete probabilities, the best decision on an expected value basis can be computed at each decision node, providing a bottom-up method for computing the best decision at the top decision node. For models with continuous probability distributions, the model's mathematical relationships generate the results for each run of a Monte Carlo simulation after a random number generator is used to select a particular value from the probability distribution for each parameter. Doing multiple runs generates a probability distribution for indicators such as revenue, profit, and market share. Those probability distributions can be used to estimate not only expected values, but also probabilities, such as the probability of making more than $X or losing more than $Y. With either discrete or continuous formulations it is possible to analyze sensitivity of the results to the probability estimates and other parameters.

In contrast, the majority of IS professionals do not conceptualize or analyze risk in the way prescribed by the decision analysis literature. For example, in 2002 the Cutter Consortium [2002] surveyed IT managers about their organizations' risk management practices. The breakdown of definitions of risk was:

- 49%: the potential for the realization of unwanted, negative consequences of an event or situation
- 22%: an uncertain condition or event that involves a negative or positive effect on achieving some objective
- 22%: any issue or event that may cause deviation from a plan
- 4%: the amount that can afford to be lost
- 2%: the differences between means and ends.

Close to half of the respondents (49%) used what Cutter calls "the traditional definition of risk", in which risk connotes negative outcomes, and risk management primarily deals with negative consequences of some event.

> "Nearly the same number (44%) are evenly split between the definition of risk that could include positive consequences of some event, as well as negative aspects. [Of those] about half are using the definition of risk that explicitly includes positive or negative effects, and half define risk as being any deviation from a plan. ...Those organizations that use formal risk management seem to favor the more traditional definition [i.e., risk as negative outcomes] over the definitions inclusive of negative and positive effects or deviation from a plan." [Cutter Consortium, 2002]

Thus, the asymmetrical "negative outcomes" approach preferred by a slim majority of the Cutter respondents differs from the symmetrical "range of outcomes" approach in much of the decision analysis literature.

A 2001 survey of members of risk management SIGs in five professional organizations related to project and risk management obtained similar results. Describing their organization's definition of risk, 54% said it focused exclusively on negative results, 34% said it included both threats and opportunities, and the remaining 13% cited uncertain events with uncertain effects or "other." In the same survey, 54% said that their organizations used risk management processes to manage threats. That 54% included 26% that used no explicit opportunity management and 28% that used separate processes for opportunity management and threat management [Roberts and Kitterman, 2002].

The divergence between the definition of risk used by the decision analysis community and the definition used by the majority of the IS community raises a quandary related to any purportedly general model of IS risk. If the model adopts a theoretically pure but unfamiliar, unintuitive, or impractical definition, its use will be limited. If the model adopts a commonly accepted but incomplete view, its results may be skewed.

What is the Role of Goals and Expectations in IS Risk?

Few of the risk models in the IS risk literature explicitly consider goals and expectations, even though goals and expectations play an important role regardless of which conceptualization of risk is used. Goals and expectations that exist prior to the time interval under consideration (which might be an accounting period or the duration of a project) are typically the basis for evaluating success. Outcomes that might be viewed as great successes under one set of goals and expectations might be viewed as dismal failures under other sets of goals and expectations. Attending to the goals and expectations that determine which outcomes are positive or negative is not only important, but essential if risk is viewed in terms of negative outcomes in relation to goals.

Goals and expectations also affect outcomes directly by setting the aspiration level of work system participants. Setting the bar higher or lower makes it easier or more difficult to succeed. Similarly, stretch goals might inspire some people to accomplish more under some circumstances or might lead to depression under other circumstances.

The mere fact of measuring success against goals and expectations also affects the meaning of risk factors and success factors and the meaning of their impact on the probabilities of positive and negative outcomes. Assume, for example, that management expects a project to generate $1 million in benefits and that a risk analysis identifies risk factors A, B, and C whose presence may make it more difficult to attain that outcome. When setting the goal, management may or may not have considered the presence of the risk factors, but after announcing the goal, management probably will be loathe to change it even if additional risk factors are identified that reduce the probability of success. Compare that situation to a different project whose expected value determined by a Monte Carlo simulation is $1 million. If the Monte Carlo simulation did not include relevant risk factors, we would assume that a follow-up simulation including the risk factors would reduce the expected value. In the first case, the risk factors present an additional challenge to project personnel but do not change management's stated goal or expectation; in the other case, the risk factors affect the expected value (whether or not management would be willing to change its goals or stated expectations). The first case represents the logic of the negative outcomes approach for analyzing risk because risk analysis is mostly about identifying and overcoming risks in order to meet the goal. Regardless of whether management holds firm to a $1 million goal in the second case, the Monte Carlo simulation will say that the expected value is less than $1 million when the risk factors are considered.

What is the Baseline for Assessing Risk?

Considering both risk factors and success factors in the analysis complicates things further. A risk analysis should contain both risk factors and success factors if both affect the probability distribution of outcomes. If a risk analysis is to produce a mathematically calculated distribution of outcomes, there must be some way to quantify the separate impacts of each risk factor and success factor, plus any interaction effects that might occur. And even assuming there is a good theoretical vehicle for computing the impacts, it is not clear how to assess the validity of the individual impact factors. Regardless of whether they were estimates based on a specific situation or regression results from a large survey, the numbers themselves would probably be difficult for most managers to understand and use.

In an even more fundamental sense, if success factors increase the probability of positive outcomes and risk factors increase the probability of negative outcomes, what is the baseline from which these effects occur? The two approaches for defining the baseline are:

1. Managers start from a baseline assumption that none of the success factors and risk factors is present, and intuitively adjust expectations based on the combined impact of all the success factors or risk factors that are present.

2. Managers start with an expectation based on their perceptions, experience, and intuition, and then adjust that expectation based on the presence or absence of each relevant success factor or risk factor.

Either approach assumes that managers are capable of identifying and combining all relevant impacts and uncertainties related to the presence or non-presence of relevant success factors and risk factors. That seems like quite a feat. Human abilities to estimate probabilities of future events are notoriously poor [Tversky and Kahneman, 1974]. Similar cognitive limits would apply if managers attempt to make quantitative estimates related to impacts of numerous, partially interacting success factors and risk factors, especially when there is no reliable way to compute or describe a real baseline.

APPROACHES USED IN EXISTING RISK MODELS

The literature contains many compilations of risk factors and clusters of risks through Delphi studies and empirical research [Barki et al., 1993; Bashein et al., 1994; Keil et al., 1998; Doherty and King, 2001; Jiang et al., 2001; Schmidt et al., 2001; Smith et al., 2001; Jiang et al., 2002; Scott and Vessey, 2002]. Only a few articles describe explicit models that explain the risk factors or use the risk factors in a risk management process. Table 2 identifies typical risk models and their limitations. Most of the models are limited to a subset of IS-related risks and provide limited guidance for risk management. We will return to these models after presenting our model.

TEMPORAL NATURE OF RISK

System-related risk manifests itself over time. Some risks exist prior to a phase of a system's life cycle; others emerge during that phase. Risk management techniques applied during a phase of the life cycle can lower risks during that phase. The risk at the end of one phase influences risk in the next phase.

Only 12 of the 46 risk studies in our literature survey specifically address the temporal nature of risks, and most of those studies focus on software development. This part of the literature typically has three limitations:

1. Some risk studies focus on specific phases of the software life cycle, without recognizing that risks in one stage can have an impact on other stages.

2. If the risk model does not include risk management, then the impacts of approaches to reduce risk are not evaluated. Risk management is an ongoing activity of identifying and

Table 2. Risk Models in the IS Literature

Type of Model	Description	Source	Limitations
Software Risk Model	Process for risk analysis and management	[Boehm, 1989; Charette, 1989; Higuera and Haimes, 1996; Kontio, 1998]	Limited to software engineering
Contingency Model	Software development project performance is influenced by fit between risk exposure and risk management	[Barki et al., 2001]	No organizing framework for risk factors. Does not distinguish between initial and emergent risks.
Socio-technological	Sociotechnical model of organizational change is used to	[Lyytinen et al., 1996]	Focuses on components internal to the firm (task,

model	classify risks by system, project, and management sources.		structure, actors, and technology), mainly during a software project's development phase
Options Model	Managing IT investment risk by choosing options that balance risk and reward. Considers risks arising outside the scope of development	[Benaroch, 2002]	Requires mapping of risks to specific options; high level of generality makes it difficult to use for identifying risks
Performance Model	Performance risk explains the effect of coordination and uncertainty on process control and product flexibility	[Nidumolu, 1995; Nidumolu, 1996]	Limited to coordination mechanisms.

reducing risk. Risk management activities should be included in a realistic model of system-related risk because recognition of risk factors encourages appropriate risk reduction tactics. For example, managers of a project that lacks a crucial skill might bring in an employee or consultant who has those skills or might change the project so that it does not require those skills. The available risk reduction tactics depend on the goals and expectations that apply. For example, a project whose goal is to minimize costs will have extra difficulty hiring expensive consultants.

3. Even when looking at a particular life cycle phase, most of these studies do not distinguish between initial and emergent risks. Distinguishing between risks that exist prior to a phase and those that emerge during a phase is important for risk management because factors that exist prior to a particular project or operational phase may be managed differently than those that emerge during that phase. Examples of pre-existing risk factors include major difficulties with previous projects and lack of knowledge about the technology that will be used. Examples of emergent risk factors include departure of key personnel during a project and need to divert resources to other purposes. New risk factors such as these can emerge due to the past and current operation of the work system or based on inherent variability, mishaps, and internal and external events that occurred or might occur during the time interval of interest.

Most of the 12 studies that addressed the temporal nature of risks were drawn from the software risk literature, which emphasizes the iterative nature of risk assessment and the importance of risk management. As an example, Table 3 shows the framework proposed by Charette [1989]. Other researchers use similar classifications with slightly varying titles. For example, Boehm [1989] calls these steps risk assessment (risk identification, risk analysis, risk prioritization) and risk control (risk management planning, risk resolution, risk monitoring).

Table 3. Risk Management Framework from Software Engineering

Risk Analysis	Risk Management
• Risk Identification: What can go wrong?	• Risk Planning: Selecting appropriate risk abatement strategies
• Risk Measurement: What is the magnitude of the risk – the expected consequence?	• Risk Controlling: Implementing the plan's control mechanism for risk aversion strategies
• Risk Evaluation: How can risks be prioritized, and how are the risk measurements related to acceptable levels of risk?	• Risk Monitoring: Refining actions and providing feedback

However, since these models focus only on software development issues, they do not include the dynamics of risk in the broader realm of projects or systems in general. Software development models are inadequate for describing, analyzing, or communicating the range of risks that are relevant to IS projects and IS in operation because many of these risks are business and organizational risks that are often considered beyond the scope of software development. We believe that frameworks and models based upon work systems [Alter, 2002; 2003] may be more useful for analyzing business and operational risks and for communicating with business customers, users, and other stakeholders who are often important sources of IS risk.

In addition to the software risk studies, Lyytinen and Nidumolu also address the temporal nature of risks in different phases of IS projects [Nidumolu, 1995; Lyytinen et al., 1996; Nidumolu, 1996; Lyytinen et al, 1998]. However, they do not explicitly consider emergent risks during a specific phase of an IS project. Lytinnen's model suggests that software risks are addressed through sequential attention shaping and intervention. The risk items are derived from postulated causal dependencies between risky incidents (events or states in the real world that can cause loss) and losses. Risk resolution techniques are based on how interventions influence risky incidents. Major variations in the socio-technical components of a system form risky incidents that increase the difficulty in estimating a development project's performance results [Nidumolu, 1995; Nidumolu, 1996].

ORGANIZATION OF RISK VARIABLES

Appendix I shows that different studies include different risk factors or components. Only a few studies attempt to organize these variables. Risk variables can apply to information systems in operation, to projects, or to special types of systems or projects. Many of the risk factors that apply to information systems in operation also apply to projects and to any work system, regardless of whether IT is involved. For example, risk factors for any work system include lack of management support, lack of required knowledge and skill, and lack of required resources. These risk factors also apply to projects, but some additional risk factors for projects do not apply to work systems in general, such as inadequate project schedule and inadequate clarity about project requirements. The organization of risk factors is the subject of our companion article [Sherer and Alter, 2004].

Even though literally hundreds of risk variables are mentioned in the literature, combining various lists from various authors does not guarantee that all risks relevant to a particular situation will be identified. Even sophisticated probabilistic risk assessments used to develop accident scenarios for complex engineered systems, such as nuclear power plants, suffer from "completeness uncertainty", uncertainty about whether all significant phenomena and relationships have been considered [Vesely and Rasmuson, 1984]. This uncertainty can arise from biases that often cloud risk identification [Tversky and Kahneman, 1974].

III. ALTERNATIVE MODELS FOR ANALYZING AND MANAGING RISK

The IS risk literature lacks a broadly accepted model of risk. Such a model would organize risk factors in a meaningful fashion, recognize that risk is measured against goals, and account for emergent risks and risk management, and hencethe temporal nature of risk.

Figure 1 presents a risk model that we believe satisfies the four criteria (clarity, practicality of use, completeness, and adaptability) identified in Section II for a general, yet broadly applicable risk model. Figure 2 is a reduced version of the more general model in Figure 1. Both are in the same basic form, except that the first model uses a "range of outcomes" approach to risk, whereas the second model uses a "negative outcomes" approach and is therefore not quite as general. In both models, system-related risk is about risks for work performed during a time interval. This work may be an entire project, a phase in a project (such as development or implementation), or the operation of a work system during the time interval in question. Risk is fundamentally about uncertainty in work performance and the resulting outcomes. Presenting

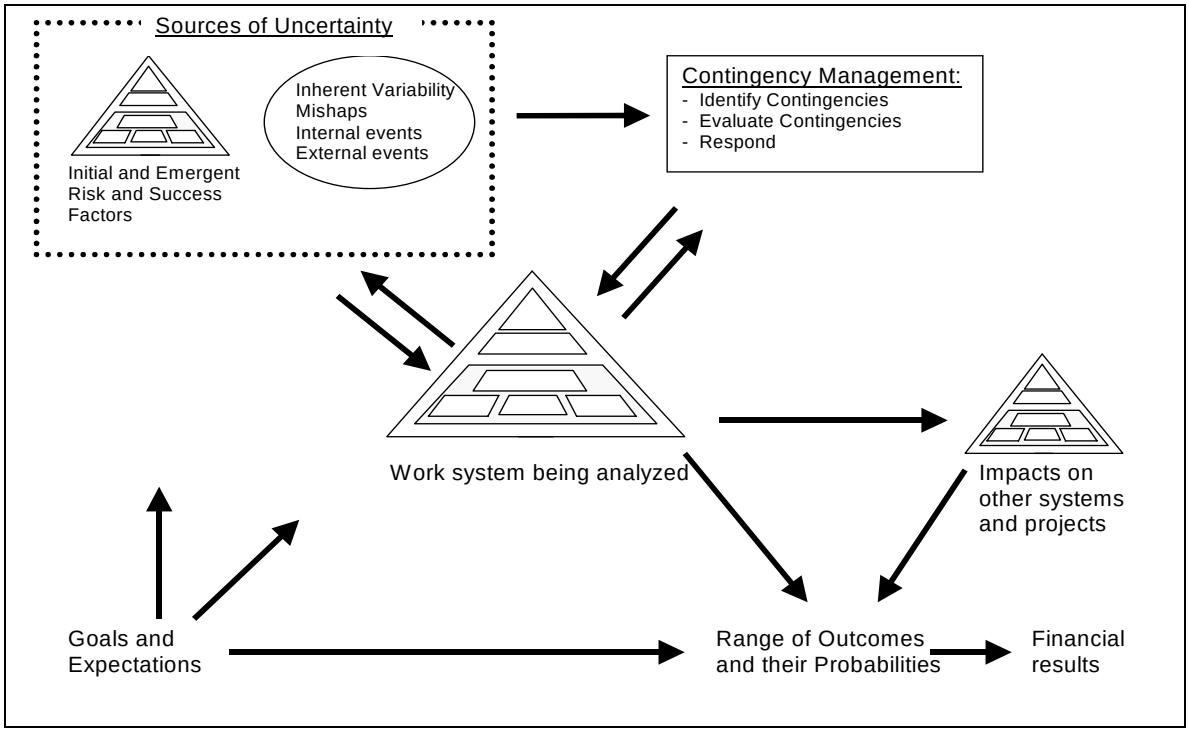

Figure 1. Model for Analyzing and Managing Contingencies Based on a "Range of Outcomes" Approach to Risk

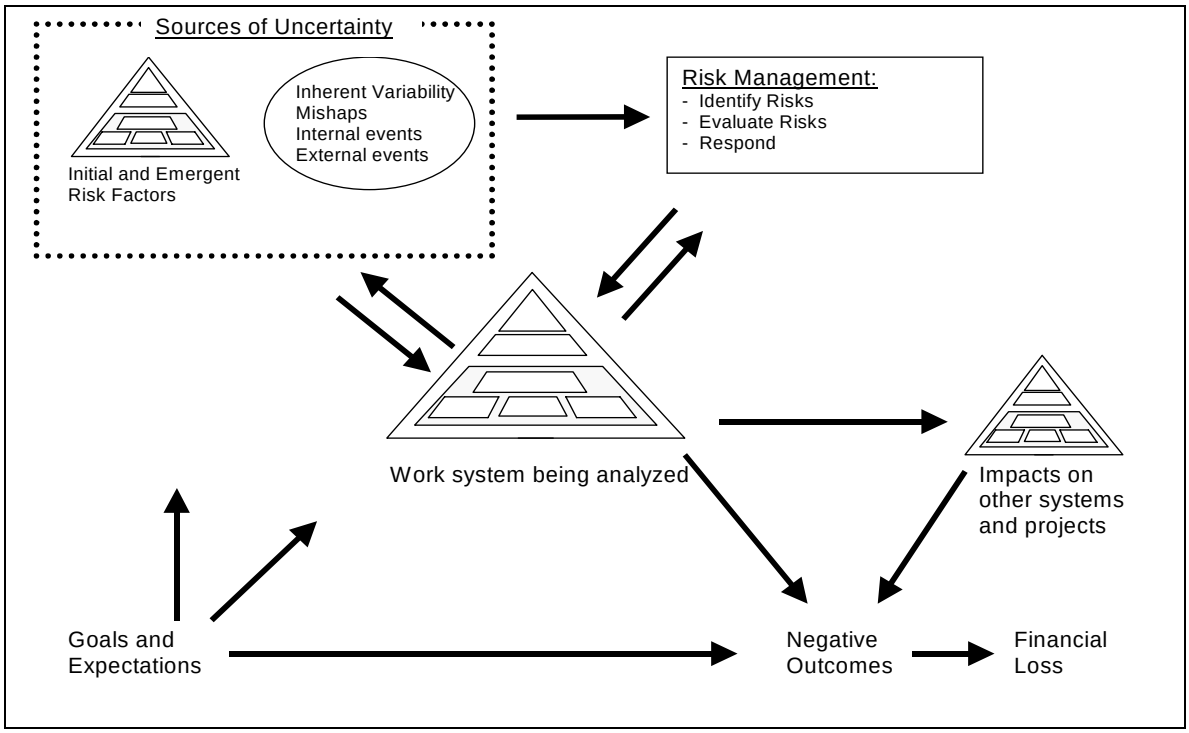

Figure 2. Model for Analyzing and Managing Risks Based on a Negative Outcomes Approach to Risk

both models reflects the distinction between the two approaches to risk and provides users a choice of which approach they prefer. The "range of outcomes" model is more general; the "negative outcomes" model is similar in flow but different in detail. Both models were designed to support further adaptation and simplification in the sense of allowing users to address or ignore specific parts of the models, and to be clear about which issues they are including or excluding.

Both models attempt to satisfy a number of goals:

- Representing risk and risk management in a much more comprehensive way than is possible with numerous, largely unrelated treatments of risk and risk factors as lengthy lists of things that could go wrong or of factors that might be correlated to negative outcomes
- Demonstrating that either version of a single risk model can cover a broad range of relevant situations
- Providing useful guidance without forcing the user to adopt a particular stance concerning the collection and use of specific quantitative or qualitative data

Either version of the model should be meaningful to potential users. For example, a general manager could use it to support risk management for an operational information system. Similarly, a software development team could use it to help organize a quantitative risk analysis based on years of data collected from a CMM (Capability Maturity Model) level 5 programming group.

Both versions of the model apply to work systems in general, as well as special cases of work systems such as information systems, projects, and more specialized cases such as ERP systems and reengineering projects.[1] Using the work system framework (rather than a representation of a software project, for example) as a central building block implies that the idea of risk management in relation to expectations and sources of uncertainty is not just about the technical work of IT professionals. The same general logic applies to risk management for almost any work system of significance.

The graphical representations in both figures illustrate relationships between facets of the model including:

- goals and expectations,
- risk factors and other sources of uncertainty,
- the operation of the work system whose risks are being managed,
- the risk management (contingency management) effort,
- the possible outcomes and their probabilities,
- the impacts on other systems,
- the resulting financial gains or losses.

---

[1] A work system is a system in which human participants and/or machines perform work using information, technology, and other resources to produce products and/or services for internal or external customers [Alter, 2003]. A work system is a general case of systems operating within or across organizations. An information system is a work system whose work practices are devoted to processing information or data. Similarly, a project is a work system designed to produce a particular product and then go out of existence. The triangular icon that appears three times in Figure 1 and in Figure 2 stands for the work system framework, a graphical representation of the nine elements included in even a rudimentary understanding of a work system. The nine elements include work practices, participants, information, technologies, products and services produced, customers, environment, infrastructure, and strategy.

The facets and relationships between them will be discussed individually, starting with the work system whose risks are being managed. For the sake of simplicity, the discussion of each facet will refer to the more general "range of outcomes" model in Figure 1. Later, after discussing the facets shared by the two models, we will return to the relative advantages and disadvantages of each model.

FACETS OF THE GENERAL MODEL

Work System Whose Risks are Being Managed

At the heart of the model in Figure 1 is a work system whose risks are being managed. The specific work system under consideration might be a work system supported by one or more information systems, or might be a specific information system, project, or supply chain that crosses organizational boundaries. (All of these are special cases of work systems.) It also might be a special case of any of them, such as a software development project or ERP implementation project. The reason for placing the work system framework at the model's core is that the same logic concerning sources of uncertainty, risk management, and outcomes applies for work systems in general, information systems, projects, and all special cases. The only difference is that the risk factors and other specifics may differ depending on the special case being considered.

Goals and Expectations

The model in Figure 1 starts with goals and expectations. The three arrows emanating from "goals and expectations" represent

- the impact of expectations and goals on the relevant risk factors and sources of uncertainty,
- the impact of goals and expectations on the level of aspiration by work system participants including managers, and
- the role of goals and expectations in evaluation of the outcomes after the time interval of interest.

Sources of Uncertainty

In addition to any relevant risk factors and success factors, the sources of uncertainty considered in risk management should include inherent variability in the situation, mishaps, internal events, and external events. Some risk factors and other sources of uncertainty (such as inherent variability) exist and can be recognized before the time interval of interest. Additional risk factors, success factors, and other sources of uncertainty (such as personnel turnover, mishaps, and organizational chaos) may emerge during the time interval. Regardless of when specific sources of uncertainty become evident, the goal of risk management is to understand and contain the uncertainties to assure that goals and expectations are satisfied. The double arrows between the work system in operation and the sources of uncertainty indicate that the uncertainties affect the operation of the work system and vice versa. For example, the risk factor inadequate expertise might cause significant delays. In turn, those delays could then cause additional uncertainties due to insufficient time to complete the work carefully.

Risk Management (Contingency Management)

The model in Figure 1 uses the term contingency management rather than risk management because a range of outcomes model places substantial emphasis on both positive and negative occurrences. Although contingency management may start with an initial risk identification and evaluation, it is assumed to continue throughout the time interval under consideration. The arrow from sources of uncertainty to contingency management says that contingency management decisions will respond to changes in the sources of uncertainty. The double arrows between contingency management and work system being analyzed indicate that contingency management affects the work system and vice versa. For example, extra control measures

introduced to reduce uncertainties due to inadequate expertise might absorb a lot of participant time, thereby potentially affecting measures of performance related to efficiency. To maintain the desired level of efficiency, managers and other work system participants might create temporary accommodations such as shifting work assignments in a way that maintains the desired rate of progress.

Other Work Systems

Information systems, projects, and other work systems never exist in isolation. Instead, they affect and are affected by other work systems. The arrow from work system being analyzed to "impacts on other systems and projects" says that positive and negative outcomes are not just direct outcomes about the work system under consideration, but may also include outcomes related to impacts on other systems and projects.

Range of Outcomes and Their Probabilities

The range of possibilities includes both disappointments and positive surprises that occur relative to the original goals and expectations. Some of the outcomes may occur during the time interval under consideration, but the totality of outcomes is evaluated after the end of the time interval.

Financial Results

Financial results are the probability distributions of outcomes, both positive and negative, expressed in monetary terms.

THE ALTERNATIVE MODEL

The alternative model in Figure 2 conceptualizes risk in terms of negative outcomes rather than the range of outcomes and related probabilities. The general form is the same as the more general model in Figure 1, but a number of the terms are different.

- Instead of risk and success factors, it only mentions risk factors.
- Instead of contingency management, it only mentions risk management.
- Instead of range of outcomes and their probabilities, it only mentions negative outcomes
- Instead of financial outcomes, it mentions financial loss.

By conceptualizing risk in terms of negative outcomes, the risk model in Figure 2 is consistent with the view of IS risk management used by the majority of organizations and by much of the IS risk literature. Based on these results from practice and from the IS literature, we believe that use of a negative outcomes approach is consistent with the way most managers think about risk related to information systems in operation and IS projects. Although the range of outcomes approach is more general and complete, we believe it has relatively little utility in most IS risk analysis because so much of the management attention in the area focuses on reducing the probability of negative outcomes relative to goals and expectations.

Another reason for adopting the negative outcomes approach is that it simplifies the entire discussion and makes management engagement more practical. If the baseline is simply a goal to be reached, risk factors need to be identified and prioritized in order to manage risks, but it is possible to skip much of the complexity related to the meaning of a mathematically computed expected value. It may be possible to quantify the risks and impacts in certain highly experienced and sophisticated software development organizations in stable environments, but such situations are rare. In typical business situations, the relevant historical data does not exist, and variability from year to year and system to system is large due to competitive forces, internal politics, and contingencies related to specific information systems.

OTHER ADAPTATIONS OF THE GENERAL MODEL

The idea of alternative models can be extended further by looking at the various facets of the models in Figures 1 and 2 and asking whether some of those facets might be eliminated or simplified to tailor the model to the user's knowledge and situation-specific needs without destroying its potential usefulness. We call this model characteristic adaptability.

Designing a risk model so that certain facets can be eliminated is consistent with the idea that genuinely useful models should be tailored to the situation users encounter. For example, a model that requires continuous probability distributions will not be used effectively in situations when there is no agreement about those distributions or when the potential users lack the training necessary to understand what probability distributions mean. Similarly, models that focus on initial conditions and ignore management actions during the time interval under consideration will be less realistic than models that consider those management actions. Table 4 identifies ramifications of eliminating or ignoring various facets of the general risk model that was shown in Figure 1.

Table 4. Implications of Eliminating or Ignoring Various Facets of the General Risk Model in Figure 1

Facet of the General Model	**Implications of Eliminating or Ignoring this Facet**
Definition of risk	The definition of risk cannot be eliminated without making the model hard to understand.
Goals and expectations	Possible adaptation: Eliminate goals and expectations from the model because the user wants to focus on the range of outcomes. Ramifications: Eliminating explicit inclusion of goals and expectations would make it impossible to use a negative outcomes approach because there would be no basis for evaluating the results. Eliminating goals and expectations would have other ramifications: … It might bring into question the meaning or intensity of some of the risk or success factors by eliminating a baseline for comparison. … It might assume unrealistic behavior by managers, who typically pay a lot of attention to goals and expectations.
Success factors	Possible adaptation: Eliminate success factors from the model Ramifications: Eliminating the success factors might skew the analysis by consciously ignoring factors that mitigate risks and that might lead to more positive results.
Risk factors	Possible adaptation: Eliminate risk factors from the model Ramifications: Risk factors can be built into the underlying assumptions and not mentioned explicitly in the analysis. It seems likely that treating risk factors as implicit will reduce their visibility and might lead to overlooking important issues.
Other sources of uncertainty	Possible adaptation: Eliminate other sources of uncertainty. Just consider risk factors in the negative outcomes approach or risk factors and success factors in the range of outcomes approach. Ramifications: If the user believes that risk factors and success factors should encompass all known sources of uncertainty, then the use of risk factors and success factors would suffice. If the user believes the opposite, eliminating other sources of uncertainty from the analysis would be acceptable only if these were

Facet of the General Model	Implications of Eliminating or Ignoring this Facet
	relatively inconsequential.
Initial risk factors	Possible adaptation: Eliminate initial risk factors because the risk analysis will start after the project has begun. Ramifications: It is hard to imagine how a risk analysis for an information system or IS project could be done without considering initial risk factors. Also, it seems unlikely anyone would want to start risk analysis after a project begins. Even if that happened and emergent risk factors appeared, many of the initial risk factors would probably still be in force.
Emergent risks	Possible adaptation: Eliminate emergent risk factors by performing the entire risk analysis must occur before the project begins. Ramifications: For some model users such as managers involved in making investment decisions, performing a complete risk analysis before the project begins can make sense because someone else will do the subsequent analysis after the project is underway.
Type of work system	Possible adaptation: Ignore the type of work system. Ramifications: Risk factors and success factors for work systems in general provide a useful first cut at the relevant risk factors and success factors for most specific systems, but it is hard to imagine why one would want to ignore risk and success factors associated with a specific system type when doing a risk analysis.
Risk management	Possible adaptation: Eliminate risk management from the model because the analysis looks at the effect of risk factors and/or success factors and assumes risk management will happen on an all things being equal basis. Ramifications: A straightforward a priori risk analysis supporting an investment decision might take this approach. Eliminating risk management from the model would not make sense, however, if the analysis were meant to cover an ongoing project.
Impacts on other systems	Possible adaptation: Eliminate consideration of impacts on other systems because that would make the analysis too broad. Ramifications: Simplifies the analysis by reducing the scope of the positive and/or negative outcomes considered in the analysis. Ignoring potentially relevant outcomes may change the results of the analysis.
Full range of outcomes	Possible adaptation: Follow some version of the model in Figure 2 and consider only negative outcomes. Ramifications: Give little or no weight to outcomes that exceed expectations in a positive direction.
Inclusion of probabilities	Possible adaptation: Exclude probabilities of events or parameter values because the probabilities cannot be estimated reliably or because disagreements about the probabilities are large. Ramifications: Excluding probabilities makes it impossible to compute expected values and restricts the types of quantitative results that a risk analysis can produce.
Range of financial results	Possible adaptation: Do not determine financial results. Just focus on positive and/or negative outcomes and actions to make the positive outcomes more likely and the negative outcomes less likely. Ramifications: The analysis cannot produce a probability distribution of financial outcomes, but can still help in identifying hazards and in supporting risk management.

COMPARISON WITH OTHER MODELS IN THE LITERATURE

Table 2 listed five risk models in the literature. The foregoing discussion of the model we propose demonstrates that our model covers a number of topics not included in the other models. Table 5 lists topics in our model and indicates whether those topics are or are not included explicitly in the models in Table 2. Table 5 is not meant as a criticism of the previous models because each of those models was designed for a particular purpose and served that purpose.

In contrast to the previous models, our risk model is more complete, adaptable, and practical for use by business managers. For example, the software risk model includes most aspects of our negative outcomes model but focuses only on software development through the point when the software meets requirements rather than when the software is used successfully as part of a new or improved work system. Our model is more useful for business managers who are concerned with managing all risks related to whatever work system is being analyzed. In contrast, Table 5 says that the contingency model, the socio-technological model, and the performance model do not explicitly consider emerging sources of uncertainty, nor do they attempt to quantify loss. These three models focus on different relationships, first between risk management and exposure, second among firm-specific factors and potential loss, and third, between uncertainty and performance. While the models are all useful to business managers, each of them is limited to a particular aspect of risk analysis. The options model addresses investment risk across a sequence of choices. It includes positive and negative financial outcomes but does not identify other sources of uncertainty in addition to specific competitive, market, and firm specific risks. Most of the models implicitly assume specific goals but provide no guidelines for measuring the impact of goals on risk.

IV. DISCUSSION AND CONCLUSIONS

This article attempted to advance the discussion of system-related risks by demonstrating steps toward better models for managing risk. It began by discussing issues related to conceptualizations of risk, the importance of goals and expectations, approaches used by different risk models, the temporal nature of risk, and the organization of risk variables. It discussed why a broadly applicable model for understanding and analyzing system- and project-related risks should define risk clearly and should include:

Table 5. Inclusion or Non-inclusion of Facets of Our Model in Previous Models

	Degree of Inclusion in the Previous Models				
Topic in our model	*Software Risk Model*	*Contingency Model*	*Socio-technical model*	*Options Model*	*Performance Model*
Goals and expectations	Implicit	Includes performance criteria	Stakeholder expectations recognized; no explicit development	Investment goals	Not explicit
Risk factors	Included	Included (technological newness, application size, expertise, application complexity, organizational environment)	Includes factors and their interactions (actors, structure, technology, task, environment)	Includes competitive and market risks in addition to firm specific risks	Requirements uncertainty and technological uncertainty
Success factors	Not included – focuses on negative outcomes	Risk management only	Not included	Implicitly included in NPV analysis of options	Not included

Other sources of uncertainty	Included	Not included	Not explicitly included	Not explicit	Not included
Temporal relationships	Included with spiral model	Scores in different stages of life cycle	Includes risk management impact	Explicitly included	Not explicit; mutual adjustments over time
Risk management	Explicitly included	Includes internal integration, formal planning, and user participation	Explicitly included	Included through choice of options	Vertical and horizontal coordination
Work system affected by changes	Software development	IS project	IS project	IS projects and IS in operation	IS projects
Impacts on other systems	Included	Not included	Not explicit	Included	Not included
Outcomes	Negative	System quality; cost gap	Negative	Positive and negative	Positive (process and product performance) and negative (overruns)
Financial results	Expected loss	Impact of potential loss (measured on a Likert scale)	Not computed	Included	Not included; project performance (process, product, overruns)

- risk factors and other sources of uncertainty,
- the temporal nature of risks,
- a clear baseline for characterizing and evaluating outcomes,
- explicit recognition of risk management activities.

It presented a new, highly adaptable risk analysis model based on those ideas, and for comparison showed an alternative model based on a different conceptualization of risk.

The discussion of topics needed in a risk management model and the presentation of alternative versions of the new risk model lead to conclusions concerning:

- the model's potential value as a step toward understanding system- and project- risk
- the impact of goals and expectations
- relative value of the negative outcomes versus range of outcomes approaches
- use of the work system framework in risk analysis
- potential value of tracing risk management activities.

We will discuss each topic in turn.

The Model's Potential Value as a Step Toward Understanding System and Project Risk

The alternative models for analyzing and managing system- and project risk in organizations (Figures 1 and 2) illustrate shortcomings of the existing IS risk literature, which relies too much on lists of risk factors and not enough on the dynamics of system-related risk. The models define risk and include risk factors and other sources of uncertainty, goals and expectations, the temporal

sequence, and risk management activities. They apply to work systems in general, as well as information systems, projects, and more specialized cases. They can be used to motivate and organize further exploration of the IS risk literature, including comparison of the issues emphasized in different parts of the literature, but there is greater potential value in developing practical risk management tools.

A possible next step would involve using this model to develop risk diagnostics and tools for improving risk management. Use of the diagnostics in any particular situation would combine relevant risks and risk factors for work systems in general plus additional risks and risk factors associated with the specific type of situation that is being managed. In developing practical risk diagnostics it would be important to verify that those diagnostics fit comfortably into risk management processes that are practical for the types of managers in the relevant situations.

Impact of Goals and Expectations

Everyday life teaches us that goals and expectations affect action. Research has shown that individuals' risk propensity affects their behaviors on software projects [Keil et al, 2000; Smith et al, 2001]. Goals and expectations also affect risk management in a variety of ways including determining the level of aspiration in doing work, creating goal-related risk factors (e.g., the risk factor of low aspirations due to slack goals vs. the risk factor of depression and cynicism due to impossible goals), and forming the basis of evaluating the results. The effects of goals and expectations on a series of issues deserve additional research:

First, is there any evidence that the degree of slack or over-reach in goals and expectations affects the way risk is conceived and managed in real situations?

Second, which risk factors and risks seem to be dependent on goals rather than other aspects of the situation?

Third, to what extent is the high failure rate of IS projects a result of how high the bar is set rather than a result of other factors ostensibly being studied?

Negative Outcomes Versus Range of Outcomes

We identified two possible conceptualizations of risk that could be used in a risk management model. The range of outcomes approach considers both positive and negative outcomes, whereas the negative outcomes approach focuses on foreseeable things that can go wrong, in some cases including the severity and probability of each negative occurrence. Most of the IS risk literature uses the latter conceptualization. In contrast, the decision science literature typically gives equal weight to positive and negative occurrences and is concerned about the distribution of outcomes around an expected value, rather than just meeting management goals and expectations. Our most general risk model is based on the "range of outcomes" conceptualization of risk, but we argued that it did not seem as useful or practical for IS risk management as the model that conceptualized risk as negative outcomes. We recognize that the "real options" planning technique of economics uses the range of outcomes, but is about sequences of investment decisions rather than risk management for projects or operational systems. The impacts of using one approach or the other in analyzing system or project risk in practice should be studied. The inclusion of contingency management also raises numerous questions about how managers perceive risks, risk factors, success, and success factors, and what types of alternatives they pursue under what circumstances. For example, how useful are current taxonomies of how managers perceive risk and success, and of the types of risk reduction and success assurance tactics they use? Taxonomies of these types should help in developing the next level of the model.

Use of the Work System Framework in Risk Analysis

We believe that using work systems as a central concept overcomes some of the limitations of previous IS risk models that focus on specific aspects of the development process (e.g. software engineering) or system usage (e.g. coordination mechanisms). The use of the work system framework in the risk models in Figures 1 and 2 serves a number of purposes that are described in more detail in the companion article [Sherer and Alter, 2004]. Because many of our arguments favor using work systems as a basic concept, it would be worth examining contrary arguments that using the concept of work system as a common denominator is undesirable because it generates less focused analysis or for other reasons.

Tracing Risk Management Activities

The risk models in Figures 1 and 2 summarize a general logic of risk management based on a combination of goals and expectations, initial and emergent risk factors, other sources of uncertainty, the operation of the work system being analyzed, and the management actions related to risk abatement. An important next step is to trace how risk management activities actually occur in different types of situations. For example, what topics do managers discuss; to what extent do they actually consider risk factors; what is the relative balance of discussions of the work system being supported versus discussions of the information or project that is attempting to support the work system? In addition to testing the validity of the new risk model, tracing how risk management actually occurs might reveal directions for improving the model and for creating tools that could help managers reduce impacts of risks they face.

REFERENCES

Alter, S. (2002). "The Work System Method for Understanding Information Systems and Information Systems Research." *Communications of the AIS* (9)6, pp. 90-104.

Alter, S. (2003). "18 Reasons Why IT-Reliant Work Systems Should Replace 'the IT Artifact' as the Core of the IS Field." *Communications of the AIS* (12)23. pp. 365-394.

Austin, R. (2001). "The Effects of Time Pressure on Quality in Software Development: An Agency Model." *Information Systems Research* (12)23, pp. 195-207.

Barki, H., S. Rivard and J. Talbot (1993). "Toward an Assessment of Software Development Risk." *Journal of Management Information Systems* (10)2, pp. 203-225.

Barki, H., S. Rivard and J. Talbot (2001). "An Integrative Contingency Model of Software Project Risk Management." *Journal of Management Information Systems* (17)4, pp. 37 (33 pgs).

Bashein, B., L. Markus and P. Riley (1994). "Preconditions for BPR Success and How to Prevent Failures." *Information Systems Management* (11)2, pp. 7-13.

Baskerville, R. and J. Stage (1996). "Controlling Prototype Development through Risk Analysis." *MIS Quarterly* (20)4, pp. 481-504.

Benaroch, M. (2002). "Managing Information Technology Investment Risk: A Real Options Perspective." *Journal of Management Information Systems* (19)2, pp. 43-84.

Boehm, B. (1988). "A Spiral Model of Software Development and Enhancement." *IEEE Computer*, pp. 61-72.

Boehm, B. (1989). *Software Risk Management*. Washington DC: IEEE Computer Society Press.

Boehm, B. and R. Ross (1989). "Theory-W Software Project Management: Principles and Examples." *IEEE Transactions on Software Engineering*, pp. 902-917.

Chan, S. (2001). "Risky E-Business." *Internal Auditor*, pp. 62-63.

Charette, R. (1989). *Software Engineering Risk Analysis and Management*. New York: McGraw Hill.

Clemons, E. K. (1991). “Evaluation of Strategic Investments in Information Technology.” *Communications of the ACM* (34)1, pp. 23-36.

Clemons, E. K. (1995). “Using Scenario Analysis to Manage the Strategic Risks of Reengineering.” *Sloan Management Review*, pp. 61-71.

Clemons, E. K., M. E. Thatcher and M. Row (1995). “Identifying Sources of Reengineering Failures: A Study of the Behavioral Factors Contributing to Reengineering Risks.” *Journal of Management Information Systems* (12)2, pp. 9-36.

Cutter Consortium (2002) "Exactly What is Risk Management?" Cutter Consortium Press Room, June 6, 2002. Accessed on March 23, 2004 at http://www.cutter.com/press/020606.html

Doherty, N. and M. King (2001). “An Investigation of the Factors Affecting the Successful Treatment of Organisational Issues in Systems Development Projects.” *European Journal of Information Systems* (10), pp. 147-160.

Gogan, J., J. Fedorowicz and A. Rao (1999). “Assessing Risks in Two Projects: A Strategic Opportunity and a Necessary Evil.” *Communications of the AIS* (1)15.

Grover, V., S. R. Jeong, W. Kettinger and J. Teng (1995). “The Implementation of Business Process Reengineering.” *Journal of Management Information Systems* (12)1, pp. 109-144.

Higuera, R. and Y. Haimes (1996). Software Risk Management. Pittsburgh, Carnegie Mellon, Software Engineering Institute, Report SEI/CMU-96-TR-012.

Jiang, J., G. Klein and R. Discenza (2001). “Information System Success as Impacted by Risks and Development Strategies.” *IEEE Transactions on Engineering Management* (48)1, pp. 46-55.

Jiang, J., G. Klein and T. S. Ellis (2002). “A Measure of Software Development Risk.” *Project Management Journal* (33)3, pp. 30-41.

Jones, C. (1994). *Assessment and Control of Software Risks*. Englewood Cliffs, NJ: Prentice Hall.

Keil, M., P. Cule, K. Lyytinen and R. Schmidt (1998). “A Framework for Identifying Software Project Risks.” *Communications of the ACM* (41)11, pp. 76-83.

Keil, M., B. Tan, K.-K. Wei and T. Saarinen (2000). “A Cross Cultural Study on Escalation of Commitment Behavior in Software Projects.” *MIS Quarterly* (24)2, pp. 299-325.

Kemerer, C. F. and G. I. Sosa (1991). “Systems Development Risks in Strategic Information Systems.” *Information and Software Technology* (33)3, pp. 212-223.

Kontio, J., G. Getto, and D. Landes (1998). Experiences in Improving Risk Processes Using the Concepts of the Riskit Method. *SIGSOFT'98, Sixth International Symposium on the Foundations of Software Engineering.*

Kumar, K. and E. Christiaanse (1999). From Static Supply Chains to Dynamic Supply Webs: Principles for Radical Redesign in the Age of Information. Proceedings of the 1999 International Conference on Information Systems, December.

Kumar, K. and H. Dissel (1996). “Sustainable Collaboration: Managing Conflict and Cooperation in Interorganizational Information Systems.” *MIS Quarterly*, pp. 279-300.

Lee, H. G. and T. Clark (1997). “Market Process Reengineering through Electronic Market Systems: Opportunities and Challenges.” *Journal of Management Information Systems* (13)3, pp. 113-136.

Loch, K., H. Carr and M. Warkentin (1992). “Threats to Information Systems: Today's Reality, Yesterday's Understanding.” *MIS Quarterly* (16)2, pp. 173-186.

Lyytinen, K., L. Mathiassen and J. Ropponen (1996). “A Framework for Software Risk Management.” *Journal of Information Technology* (11), pp. 275-285.

Lyytinen, K., L. Mathiassen and J. Ropponen (1998). “Attention Shaping and Software Risk - a Categorical Analysis of Four Classical Risk Management Approaches.” *Information Systems Research* (9)3, pp. 233-255.

McComb, D. and J. Y. Smith (1991). “System Project Failure: The Heuristics of Risk.” *Journal of Information Systems* (8)1, pp. 25-34.

McFarlan, W. (1981). “Portfolio Approach to Information Systems.” *Harvard Business Review*, pp. 142-150.

Mohan, L., W. Holstein and R. Adams (1990). “EIS: It Can Work in the Public Sector.” *MIS Quarterly*, pp. 435-448.

Moynihan, T. (2002). “Coping with Client-Based "People Problems": The Theories of Action of Experienced IS/Software Project Management.” *Information and Management* (39), pp. 377-390.

Nidumolu, S. (1995). “The Effect of Coordination and Uncertainty on Software Project Performance: Residual Performance Risk as an Intervening Variable.” *Information Systems Research* (6)3, pp. 191-219.

Nidumolu, S. (1996). “A Comparison of Structural Contingency and Risk-Based Perspectives on Coordination in Software Development Projects.” *Journal of Management Information Systems* (13)2, pp. 77-113.

Rainer, R., C. Snyder and H. Carr (1991). “Risk Analysis for Information Technology.” *Journal of Management Information Systems* (8)1, pp. 129-147.

Rainer, R. K. and H. Watson (1995). “The Keys to Executive Information Systems Success.” *Journal of Management Information Systems* (12)2, pp. 83-98.

Richmond, W. B. and A. Seidmann (1993). “Software Development Outsourcing Contract: Structure and Business Value.” *Journal of Management Information Systems* (10)1, pp. 57.

Roberts, B. and R. Kitterman (2002) "Risk Management Working Group" *INCOSE Insight: A Publication of the International Council on Systems Engineering*, (5)1, April, pp. 31-33. Accessed on Mar. 23, 2004 at http://www.incose.org/insight-archive/posted/vol-5-issue-1.pdf

Rockart, J. F. and A. D. Crescenzi (1984). “Engaging Top Management in Information Technology.” *Sloan Management Review*, pp. 3-16.

Schmidt, R., K. Lyytinen, M. Keil and P. Cule (2001). “Identifying Software Project Risks: An International Delphi Study.” *Journal of Management Information Systems* (17)4, pp. 5-36.

Scott, J. and I. Vessey (2002). “Managing Risks in Enterprise Systems.” *Communications of the ACM* (45)4, pp. 74-81.

Sherer, S. (1992). *Software Failure Risk: Measurement and Management*. New York: Plenum Press.

Sherer, S. A., M. Ray and N. Chowdhury (2002). Assessing Information Technology Investments with an Integrative Process Framework. *Proceedings of 35th International Conference on System Sciences, Hawaii.*

Sherer, S.A. and S. Alter (2004). "Information Systems Risks and Risk Factors: Are they Mostly about Information Systems?" *Communications of AIS (14)2,* pp. 29-62

Smith, H., J. McKeen and D. S. Staples (2001). “Risk Management in Information Systems: Problems and Pitfalls.” *Communications of the AIS* (7)13.

Straub, D. and R. Welke (1998). “Coping with Systems Risk: Security Planning Models for Management Decision Making.” *MIS Quarterly*, pp. 441-469.

Tversky, A. and A. Kahneman (1974). "Judgement under Uncertainty: Heuristics and Biases." *Science* (185), pp. 1124-1131.

Vesely, W. E. and D. M. Rasmuson (1984). "Uncertainties in Nuclear Probabilistic Risk Analyses." *Risk Analysis* (4)4, pp. 312-322.

Viehland, D. (2002). ""Risk E-Business": Assessing Risk in Electronic Commerce." *Decision Line*.

Vitale, M. (1986). "The Growing Risks of Information Systems Success." *MIS Quarterly* (10)4, pp. 327-336.

Yourstone, S. and H. Smith (2002). "Managing System Errors and Failures in Health Care Organizations: Suggestions for Practice and Research." *Health Care Management Review* (27)1, pp. 50-61.

APPENDIX I: A SAMPLE OF THE IS RISK LITERATURE

Source	***# of variables***	***Risk Variables***	***Model /Approach***	***Risk Definition***	***Type of System or Project***	***Temporal Variables***
[Austin, 2001]		Shortcuts	Model to analyze the effects of time pressure on quality	Component	Software projects	
[Barki et al., 1993]	35	Technological newness, application size, lack of expertise, application complexity, organizational environment	Survey	Project uncertainty X Magnitude of potential loss	IS project	Scores in different stages of life cycle
[Barki et al., 2001]	23	Technological newness, application size, lack of expertise, application complexity, organizational environment	Software development project performance is influenced by fit between risk exposure and risk management	Project uncertainty X Magnitude of potential loss	IS project	
[Bashein et al., 1994]	3	Lack of sustained management commitment, unrealistic scope and expectations, resistance to change	Survey of BPR consultants	Not defined	BPR projects	
[Baskerville and Stage, 1996]	28	Developers, users, application domain, problem domain, computer system, development environment	Explicit risk management enables risk resolution strategies to be put in place before prototyping.	Severity and probability	IS prototyping project	Iterative with prototypes
[Benaroch, 2002]	3	Firm specific risks, competitive risks, market risks	Managing IT investment risk by choosing options that balance risk and	Components	IS projects and IS in operation	

			reward			
[Boehm, 1989]	10	Personnel shortfalls, unrealistic schedules and budgets, continuous stream of requirements changes, shortfalls in components, task, straining capabilities	Project management theory to make everyone a winner	Probability times loss	Software project	Risk analysis followed by risk manage-ment; spiral model
[Boehm and Ross, 1989]			Model with steps for risk assessment (identification, analysis, prioritization) and risk control (management planning, resolution, and monitoring)	Probability times loss	Software project	Risk analysis followed by risk manage-ment
[Boehm, 1988]	10	Personnel shortfalls, unrealistic schedules and budgets, continuous stream of requirements changes, shortfalls in components, task, straining capabilities	Software process model	Probability times loss	Software project	Spiral model
[Chan, 2001]		Credit, market, liquidity, insurance, operational, reputational, strategic, competitive, regulatory, systemic	Risk framework	Components	E-business operation	
[Charette, 1989]			Approach to software engineering analysis and management	Probability times loss	Software project	Risk analysis followed by manage-ment
[Clemons, 1995]	2	Functionality risk, political risk	Scenario analysis to manage risks of reengineering	Risk Components	Reengineer-ing Project	
[Clemons et al., 1995]	5	Political risk, financial risk, technical risk, functionality risk, project risk	Identifying reengineering risks	Risk components	Reengineer-ing project	
[Clemons, 1991]	5	Financial risk, technical risk, functionality risk, project risk, systemic risk	Balance and manage different risks	Risk components	Strategic info systems project	
[Doherty and King, 2001]	2	Organizational, technical	Survey identifying treatment of organizational vs. technical issues	Organization-al issues, not risk	IS project	Project phases
[Gogan et al., 1999]	5	Time constraints, system interdependence, project size, project	Adds two new variables to McFarlan's model; case studies	Likelihood and consequence	IS project	

		structure, technology familiarity				
[Grover et al., 1995]		Management support, technology competence, process delineation, project planning, change management, project management	Identification and severity of problems	Not defined as risk; problems	Reengin-eering	
[Higuera and Haimes, 1996]	64	Software risk taxonomy by class, element, and attribute	Software risk taxonomy	Probability times consequence	Software project	Risk manage-ment paradigm
[Jiang et al., 2001]	34	Technological acquisition, application size, lack of team's application expertise, lack of user support, lack of clarity of role definitions, lack of user experience	Instrument to measure software development risk	Risk factors	IS project	
[Jiang et al., 2002]	34	Technological acquisition, application size, lack of team's application expertise, lack of user support, lack of clarity of role definitions, lack of user experience	Risk reduction strategies involving behavioral aspects are more influential in risk reduction than those aimed at technical risks.	Risk factors	IS project	
[Jones, 1994]	63	See contents	For each factor, provides information on severity scales, frequency, occurrence susceptibility and resistance, root causes	Risk Factors	Software project	
[Keil et al., 1998]	11	Lack of top mgt commitment, failure to gain user commitment, misunderstanding requirements, lack of adequate user involvement, failure to manage end user expectations, changing scope/objectives, lack of required knowledge/skills, lack of frozen requirements, introduction of new technology, insufficient staffing, conflict between user	Risk categorization framework based upon perceived level of control and perceived relative importance	Risk Factors	IS project	

		departments				
[Keil et al., 2000]		Risk propensity, risk perception	Model that considers the affect of risk propensity, level of sunk cost, and risk perception on willingness to continue a project	Probability that undesirable outcomes will occur	IS project	
[Kemerer and Sosa, 1991]	15	Concept, technical infeasibility, funding, market creation, telecommunica-tions, vendors, inter-organizational systems, leading edge, competitor copying, over subscription, maintenance, exit barriers, available funding, technological sophistication, organizational flexibility	Identification of barriers to successful definition, development, and maintenance of strategic information systems	Scores on risk factors	SIS project or operation	
[Kumar and Dissel, 1996]		Economic, technical, socio-political	Identification of risks in different types of IOIS	Risk components	Inter-organ-izational info systems	
[Lee and Clark, 1997]		Transaction risks	Transaction risks are analyzed to identify adoption barriers	Risk component	Reengin-eering	
[Lyytinen et al., 1998]	4+	Task, structure, actors, technology, and interdependencies among these	Use a sociotechnical model of organizational change to classify risks – system, project, and management sources.	Risk Factors (sources)	IS project	Risk manage-ment reduces risks
[Lyytinen et al., 1998]	4+	Task, structure, actors, technology, and interdependencies among these	A contingent, contextual and multivariate view of software development risk can help shape management attention	Risk Factors (sources)	IS project	Managers address risks through sequential attention shaping and intervention
[Mohan et al., 1990]			Approach to minimize risk	Not defined	EIS project	
[Moynihan, 2002]	7	Unrealistic customer expectations, lack of real customer ownership, disagreement amongst customer's people on project goals, personal deficiencies on part of customer's PM, user resistance, presence of hidden agendas,	Coping with client – based people problems requires explicitness, clarity, and formality	Factors	IS project	

		nasty politics by customer				
[McFarlan, 1981]	3	Size, experience, structure	Framework	Exposure to consequences	IS project	
[McComb and Smith, 1991]		Technical, human, planning, executing	Framework with heuristic guidelines	Risk Factors	IS project	
[Nidumolu, 1995]	5	Process control, product flexibility, requirements uncertainty, vertical coordination, horizontal coordination, performance risk	Vertical control reduces performance risk and increases control over the process whereas horizontal coordination leads to flexible software applications. Performance risk mediates the effect of vertical coordination and requirements uncertainty on process control.	Difficulty in estimating outcome	IS project	Mutual adjustments over time
[Nidumolu, 1996]	5	Process control, product flexibility, requirements uncertainty, vertical coordination, horizontal coordination, performance risk	Performance risk is an alternative to fit that explains the effect of coordination and uncertainty on process control and product flexibility	Difficulty in estimating outcome	IS project	Adjust over time
[Rainer and Watson, 1995]	23 dev 38 ops	Professional issues, executive/profess-ional relationship, executive involvement issues, information delivery issues, information quality, impact on executive work, EIS functions, ease of use	Rank ordered keys to successful development	No definition	EIS project and operation	
[Rainer et al., 1991]	22	Physical threats, unauthorized physical or electronic access, authorized physical or electronic access	Risk analysis method that employs a combination of qualitative and quantitative methodologies	Loss expectancy	Operation	
[Richmond and Seidmann, 1993]			Two-stage contracting model for software design and development	No definition	Software project (out-sourcing)	
[Scott and Vessey, 2002]	26	Organizational context, IS context, project	Risk factors in ERP implementations	Risk Factors	ERP project	
[Schmidt et al., 2001]	53	Corporate environment, sponsorship, ownership, relationship management, project	Authoritative list of common risk factors obtained from Delphi survey in 3 countries	Risk Factors	IS project	

		management, scope, requirements, funding, scheduling, development process, personnel, staffing, technology, external dependencies, planning				
[Sherer, 1992]		Software failure	Process for measuring software risk	Probability times loss	Software operation	
[Smith et al., 2001]	7	Financial risk, security risk, technology risk, people risk, information risk, business process risk, success risk	Identification of risk components from focus group	Components	IS project	
[Straub and Welke, 1998]		Organizational environment, IS environment, individual characteristics	Approach that deals with problem that managers often lack knowledge of controls	Probability times loss	Operations	
[Viehland, 2002]	3	Competitive risk, transition risk, business partner risk	Identifies risk in ecommerce	Components	Operations (e-commerce)	
[Vitale, 1986]		Changing basis of competition, raising entry barriers, increasing switching costs, changing balance of power, developing new products	Framework to assess risks	Components	Operation of competitive information systems	
[Yourstone and Smith, 2002]		Active failures, latent failures	Conceptual model for managing system errors that distinguishes between active and latent failures	Not defined	Operation (health care systems)	

ABOUT THE AUTHORS

Steven Alter is Professor of Information Systems at the University of San Francisco. He holds a B.S. in mathematics and Ph.D. in management science from MIT. He extended his 1975 Ph.D. thesis into one of the first books on decision support systems. After teaching at the University of Southern California he served for eight years as co-founder and Vice President of Consilium, a manufacturing software firm that went public in 1989 and was acquired by Applied Materials in 1998. His many roles at Consilium included starting departments for customer service, training, documentation, technical support, and product management. Upon returning to academia, he wrote an information systems textbook that is currently in its fourth edition, *Information Systems: Foundation of E-business*. His research for the last decade concerned developing systems analysis concepts and methods that can be used by typical business professionals and can support communication with IT professionals. His articles appear in *Harvard Business Review, Sloan Management Review, MIS Quarterly, Interfaces, Communications of the ACM, Communications of the AIS, CIO Insight, Futures, The Futurist,* and many conference transactions.

Susan A. Sherer is the Kenan Professor of IT Management, Program Director of Information Systems, and co-director of the Center for Value Chain Research at Lehigh University. Sherer received her Ph.D. in Decision Sciences from the Wharton School of the University of Pennsylvania, M.S. Industrial Engineering from SUNY Buffalo, and B.S. Mathematics from SUNY Albany. Her research interests include software failure risk, managing information systems risks, inter-organizational information systems, and IT benefit justification. She is the author of *Software Failure Risk*: *Measurement and Management,* as well as articles in a variety of journals including *Information and Management, Information Systems Frontiers, Journal of Information Systems, International Journal of Electronic Commerce,* and *Communications of AIS.* Prior to moving into academia, Dr. Sherer managed projects for several manufacturing companies including Leeds & Northrup Company and Union Carbide Corporation.

Communications of the Association for Information Systems

ISSN: 1529-3181