PROJECT RISK MANAGEMENT WITHIN INFORMATION SYSTEMS

Snyder, Rell
National University

ABSTRACT
Project risk management has been recognized as a means for analyzing and responding to risks in complex, multi-stage undertakings. However, in spite of the critical role that information systems have played in recent organizational life, there has been slowly increasing research literature currently available as to the practice of project risk management in relation to information system (IS) development. The reasons for the lack of attention paid to IS development project risk management remain unknown. An overview is provided on IS development as well as risk maturity that may prove useful for project management professionals. This paper revisits this topic (Snyder, 2011) to evaluate future progress in the success of IS projects.

INTRODUCTION
Organizations today are much more concerned about the effects of competition than they were in the past; therefore, no organization would like to stand the risk of being overtaken by other competitors on the same playing ground with equal opportunities (Achimuga, Babajide, Oluwaranti, Oluwagbemi, Gambo, 2010). Project risk management has increasingly received attention as a critical process in responding to ongoing failures in project management. According to a study by Wet and Visser (2013) “global research indicates that the success rate of software projects worldwide is currently very low, and has been low for the past few decades. The application of risk management has improved the success rate of software projects worldwide.” This paper provides a review of current literature on information system development that may prove useful for management professionals interested in initiating project risk management efforts within IS projects. An overview is provided of the underlying philosophies and principles of IS development, followed by a brief overview of the literature on risk mature organizations/projects. This body of knowledge may be useful in future efforts to investigate and document current practices in IS development project risk management.

NEED FOR SYSTEMS RISK MANAGEMENT
The role of IT in business activities has been more and more important; besides, the amount of its investment is also increasing. The key of operating businesses more effectively is to base on the operating principles and to play the role of IT systems. The application of IT systems can not only apply to business operations and maintenance, but also to social services and business competition (Zhe, Yunfei, Maosheng, 2010).

With the proliferation of computers and near universal network connectivity, the field of information technology has continued to shift from a focus on stand alone personal computing to developing solutions to support people and the systems within which they
work in collaboration activities. Network technology and global information systems have provided the opportunity for people to conduct work in a variety of locations, continuing to further increase the appeal of IT initiated collaboration and communication. As well, organizational systems have expanded, moving from a localized to an increasingly global presence.

Increasing competition and advancing information and communication technologies have forced organizational systems to operate within ever more complicated, turbulent environments, such as, e-commerce based business to business (B2B) supply chains. To adjust to the volatile environment, theorists argue for the need to establish organizational paradigms that promote flexibility (Drucker, 1999; Davenport & Prusak; 1998) as well as organizations having access to information on risks that can lead to project failures and solutions that can prevent such failures (Artto & Hawk, 1999). The flexibility to continuously assess programs and operations and change procedures to meet shifting customer/consumer expectations allows an organization to thrive in a volatile and turbulent environment while project risk management offers organizations the ability to avoid and prevent potential risks that can lead to project and organizational failure.

The unpredictable and nature of software development creates risks to organizations. The Standish Group (2009) reports that only 32 percent of information systems projects are successful based on success criteria of:

1. Completed on time
2. Completed within budget
3. Completed with the required functionality

Accompanying these growing demands and expectations is ongoing concern regarding the number of information system application development projects that fail (e.g., Kharbanda & Stallworthy, 1983; Standish, 1995; Kharbanda & Pinto, 1996; Artto, 1997; Pinto, 1997; Hoffman & King, 1997; Ulfelder, 2001). According to the Project Management Institute (2000), the major reasons projects fail are as follows:

1. Insufficient early planning
2. Unrealistic project plan
3. Scope underestimated
4. Customer / management changes
5. Insufficient contingency planning
6. Inability to track progress
7. Inability to detect problems
8. Insufficient number of checkpoints
9. Staffing problems
10. Technical complexities
11. Priority Changes
12. No commitment to plan by team
13. Uncooperative support groups
14. Sinking team spirit
15. Unqualified project personnel

Laudon and Laudon (2014) state to develop an effective systems development plan an organization must have a clear understanding of both its short and long term information requirements. Companies should look at the portfolio of their projects in terms of benefit verses risk. Certain projects should be developed rapidly while others should be avoided.

According to Turbit (2013) risk need to be quantified in two dimensions. The impact of the risk needs to be assessed. The probability of the risk occurring needs to be assessed. For simplicity, rate each on a 1 to 4 scale. The larger the number, the larger the impact or probability.

The figure below by Laudon and Laudon (2014) show a method of doing Portfolio Analysis.

<table>
<thead>
<tr>
<th>Benefits to the firm</th>
<th>High</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Cautiously examine</td>
<td>Identify and Develop</td>
</tr>
<tr>
<td>Low</td>
<td>Avoid</td>
<td>Routine projects</td>
</tr>
</tbody>
</table>

Laudon and Laudon (2014) also state a scoring model can be useful where many criteria must be evaluated. The model assigns weights to features of the system then calculates the weighted totals. According to Turbit (2013) risk need to be quantified in two dimensions. The impact of the risk needs to be assessed. The probability of the risk occurring needs to be assessed. For simplicity, rate each on a 1 to 4 scale. The larger the number, the larger the impact or probability.

The current direction of the risk management field is to promote learning and creative ways to conduct project risk management for organizational learning. Project management efforts have led to a growing conceptualization and understanding of the process of assessing and identifying risks to be used in the introduction of experience-based solutions for avoiding and preventing risk damage. According to these authors, the risk knowledge bases are expected to grow as experience about risks and potential risk responses are recorded during project executions. The resulting knowledge base will eventually provide assimilated information to organizations and those engaged in project risk management with access to information and understanding about risks in real time.

**DEVELOPMENT PRINCIPLES**

According to Achimuga, Babajide, Oluwaranti, Oluwagbemi, Gambo (2010) the outcomes of an IS project are identified as the success of 1) IS implementation, 2) IS investment, and 3) IS functionality. IS Evaluation should not work only as a justification mechanism but as a tool for experience learning. During the IS development process, feedback from the evaluation process should lead to corrective actions if necessary.
These actions might include, for example, a change in the information system
development or procurement strategy, or a change in the resources that are given to the
project.

IS development has emerged as a pervasive new technology with a growing dependence
and reliance on effective IS development methodologies and models. As suggested by
Birnbaum (1997), most technology passes through four stages of development:

1. It begins within labs as the curiosity factor encourages its emergence;
2. In the early stages, it is used by a small number of specialists to solve a
   particular problem;
3. Over time, it becomes manufacturable, and commonplace, but still
   requires extensive specialized training, and is used only by a relatively small
   number of specialists;
4. Eventually, it becomes pervasive, and viewed as part of the natural world
   by most people.

As IT has continued to grow rapidly, there has been an increasing demand for IS
development innovation to be driven by inter-disciplinary research. This need, according
to Rasegard (1997), has been brought about by the desire to achieve higher usability. As
such, information systems need to be able to satisfy requirements in several dimensions,
including:

1. Appropriate functionality: the system solves the right problems, communicate its purpose, and performs the work that has to be carried out.
2. Ergonomic: appropriate physical fit, feel, shape and size.
3. Cognitive fit: the product provides functionality, feedback, support for learning, and accessible understanding.

According to IEEE Standard 1540 for software management (2001) to evaluate the
risk management process this activity should include the capture of risk management
information, have the ability to access and improve the process and create lessons learned.
DEVELOPMENT APPROACHES
According to Laudon and Laudon (2014) information technology can promote various degrees of organizational change. The four types include: automation, rationalization, redesign and paradigm shifts. “The most common forms of organizational change are automation and rationalization. These are relatively slow moving and slow changing strategies present modest returns but little risk. Faster and more comprehensive change – such as redesign and paradigm shifts – carries high rewards but offers substantial chances of failure.

With the growing recognition that IS plays a major role in insuring the success of virtually all organizations in business, government, and defense, awareness has also increased that such success is dependent on the availability and correct functioning of large-scale networked information systems of astonishing complexity. Consequently, the SDLC model has become the context for further development of IS development requirements that focus on system survivability (i.e., end products that survive).

As delineated in materials provided by the Carnegie Mellon Software Engineering Institute (2002), survivability is the capability of a system to fulfill its mission in a timely manner, even in the presence of attacks or failures. As further clarified by the Institute, survivability moves beyond the realm of security and fault tolerance with a focus on delivery of essential services. On the basis of a survivability perspective, the delivery of essential services remains critical, even when systems are penetrated and/or experience failures and rapid recovery of full services when conditions improve.

According to the Institute, survivability addresses highly distributed, unbounded network environments that lack central control and unified security policies. The focus of IS development when survivability is a critical component is on insuring three key
capabilities of IS. Therefore, IS development requirements for development and implementation are those which help to insure that the final product has the following capabilities in order to be successful:

1. Resistance: the capability of a system to repel attacks
2. Recognition: the capability of a system to detect attacks as they occur and to evaluate the extent of damage and compromise
3. Recovery: the capability of the system to maintain essential services and assets during attack, limit the extent of damage, and restore full services following attack.

The Carnegie Mellon Software Engineering Institute (2002) has developed an IS development approach, the Survivable Systems Analysis (SSA) method (formerly the Survivable Network Analysis method), that focuses on the application of requirements in development and implementation to insure an end product capable of survivability. According to the Institute, SSA is a practical engineering process that permits systematic assessment of the survivability properties of proposed systems, existing systems, and modifications to existing systems. As delineated by the Institute, the SSA process is composed of four steps, as follows:

1. System Definition: developing an understanding of mission objectives, requirements for the current or new system, structure and properties of the system architecture, and risks in the operational environment
2. Essential Capability Definition: identification of (as based on mission objectives and failure consequences) essential services (i.e., services that must be maintained during attack) and essential assets (i.e., assets whose integrity, confidentiality, availability, and other properties must be maintained during attack) as characterized by usage scenarios, which are traced through the architecture to identify essential components whose survivability must be ensured
3. Compromisable Capability Definition: selection of intrusion scenarios based on assessment of environmental risks and intruder capabilities and identification of corresponding compromisable components (components that could be penetrated and damaged by intrusion)
4. Survivability Analysis: analysis of IS components and the supporting architecture for the key survivability properties of resistance, recognition, and recovery; the production of a survivability map that enumerates, for every intrusion scenario and corresponding compromised component effects, the current and recommended IS architecture strategies for resistance, recognition, and recovery.

As suggested by the Center for Technology in Government (CTG) (1998), while the SDLC has been used extensively, it has a number of associated problems. According to CTG, SDLC has been criticized for having rigid design and inflexible procedures. Consequently, as addressed by CTG, SDLC fails to account for the fact that real projects rarely follow the sequential flow that the model proposes. Because the SDLC model is a sequential process, any variations in its process create problems for the developer. As
noted by CTG, most IS development projects experience a great deal of uncertainty about requirements and goals in the beginning phase, and it is therefore difficult for customers to identify criteria on a detailed level. The SDLC model does not accommodate this natural uncertainty very well. The end result is that implementation of the SDLC model can be a long, painstaking process that fails to provide a working version of the system until late in the process. Thus, such criticisms have led to alternative IS development processes that offer faster results and greater flexibility, and require less up-front information.

One such model is that known as the Prototyping model. According to the CTG (1998), the Prototyping model was developed as a means to compensate for some of the problems identified as associated with the SDLC model. The Prototyping model is based on the assumption that it is often difficult to know all IS requirements during the beginning phases of a project. Through the application of the Prototyping model in IS development, the developer builds a framework of the proposed system and presents it to the customer for consideration as part of the development process. The customer in turn provides feedback to the developer, who goes back to refine the prototype to incorporate the additional information. This collaborative process continues until the prototype is developed into a system that can be implemented. As reported by the CTG, the Prototyping model is probably the most imitated IS development. Variations of the model include: Rapid Application Development (RAD) and Joint Application Development (JAD).

According to the CTG (1998), overall criticisms of the Prototyping model have generally fallen into the following categories:

1. False expectations: Prototyping often creates a situation where the customer mistakenly believes that the system is “finished” when in fact it is not.
2. Poorly designed systems: Because the primary goal of Prototyping is rapid development, the design of the system can sometimes suffer with the system built in a series of “layers” without a global consideration of integration of all other components. Attempting to retroactively produce a solid system design can sometimes be problematic.

A third IS development model, the Exploratory Model, represents an effort to move further away from an IS development framework in which requirements are not necessary in development and implementation activities. According to the CTG (1998), the Exploratory model is most often used in fields such as astronomy or artificial intelligence because much of the research in these areas is based on guess-work, estimation, and hypothesis. The steps in the Exploratory Model involve initial specification development, system construction modification, system test and system implementation when modifications and testing are indicative of a finished product. According to the CTG, criticisms of the Exploratory model include: its being limited to the use of very high-level languages, such as LISP; difficulty in measuring or predicting cost effectiveness; and final product inefficiency.
As indicated by the CTG (1998), the Spiral model represents an incorporation of the best features of the SDLC and Prototyping models, while introducing a new risk-assessment component. The term “spiral” is used to describe the process that is followed as the development of the system takes place. Similar to the Prototyping model, an initial version of the system is developed, and then repetitively modified based on input received from customer evaluations. However, within the Spiral model, the development of each version of the system is carefully designed using the steps involved in the SDLC model. Each version of the development system is evaluated to assess associated risk and to determine if the IS development process should continue. The steps implemented within the Spiral model include planning, risk assessment, engineering, and, customer evaluation.

According to the CTG (1998), few criticisms have as of yet been directed at the Spiral model, due to its relatively recent inception. There has been an indication that the risk assessment component of the Spiral model provides both developers and customers with a measuring tool that earlier models do not have.

As is evident, the philosophies underlying IS development models and the emergence of models have been in a process of ongoing development. As the requirements for IS development change, thanks to rapidly emerging IS/IT technologies and methodologies, as well as customer demands, the rules associated with IS development and IS development models also are altered to meet the current needs of companies, developers and customers. On the basis of the history of IS development, it can be expected that such changes will continue to occur as further efforts are directed towards the development of newer and more practical IS development models.

KNOWLEDGE AND STANDARDS
Conflict is a pervasive phenomenon during the information systems (IS) development process. The sources of conflict during the IS development process include hostility and jealousy, poor communication, user resistance, frustration and low morale, lack of trust and understanding, personality diversity, and different expectations. The critical role played by conflict in IS development projects is widely acknowledged in the IS. Unfortunately, our understanding of the impact of conflict on IS project outcomes is still limited due to conflicting results reported in the literature (Liu, Chen, Klein Jiang, 2009).

Systems differ in their size, scope and complexity as well as their organizational and technical components (Laudon and Laudon (2014). The level of project risk is influenced by size, structure and technical expertise of the IS staff and project team.

According to Feldman (2010), the practice of enterprise project management is finally getting broad respect, not just lip service. Seven out of 10 companies use formal project management methodologies, our new InformationWeek Analytics survey finds. Pay for project managers was on the rise last year, even as pay for most IT pros was flat. Sixty-one percent of the managers we surveyed see the Project Management Institute's project management professional - PMP - certification as important to their companies. Most
companies have some project management methodology in place, and that's part of the problem - if you're not actively questioning your approach, looking for weak spots, and comparing it with other options, it'll creep along in whatever direction it's already headed.

According to Bataller (2011), while just 3% of respondents to our survey say a CRO is the primary owner of the IT risk management program within their companies, we think that within a few years, the role will be commonplace, especially in large enterprises. However, to bring everyone together, the CRO must be able to form an agile organization that can dodge and weave and evolve with the regulatory climate, attacker landscape, budgetary cycles, and industry dynamics. The CRO must have a vision compelling enough to silence the inevitable naysayers and gain cooperation from people with many different priorities.

The PMBOK Guide (2000) provides the most extensive body of knowledge and standards regarding project risk management. As defined within the guide, risk management represents the systematic process of identifying, analyzing and responding to potential project risk. The risk management process provides opportunity to maximize the probability and impact of positive project outcomes while minimizing the probability and consequences adverse outcomes. As further explained within the guide, project risk is an uncertain event or condition that, if it occurs, has a positive or negative effect on a project objective. Additionally, as suggested within the guide, it is important to recognize that a risk has a cause and, if it occurs, an impact.

According to information provided in the PMBOK Guide (2000), the major processes associated with risk management include the following:

1. Risk Management Planning: the process by which a plan is developed as to how to approach and implement risk management activities for a project.
2. Risk Identification: the process by which risks that may potential impact the project are identified and characterized.
3. Qualitative Risk Analysis: the process by which a qualitative analysis of risks and conditions is conducted with the results being used to prioritize the effects of risks on project objectives.
4. Quantitative Risk Analysis: the process by which the probability and impact of risks are measured with results being used to estimate implications for project outcomes.
5. Risk Response Planning: the process by which procedures and techniques to enhance opportunities and to reduce threats to the project’s objectives are identified and/or developed.
6. Risk Monitoring and Control: the process by which residual risks are monitored while identifying new risks, executing risk reduction plans and evaluating their effectiveness through the project life cycle.

Interest Group, and the UK Association for Project Management Risk Specific Interest Group, describes a Risk Management Maturity Model (RMMM) with four levels of capability maturity, each linked to specific attributes. As suggested within the report, organizations and projects can use RMMM to assess and determine their current level of risk management capability maturity, identify realistic targets for improvement, and produce action plans for developing or enhancing their risk management capability maturity level. As explained within the report, RMMM represents a very simplified maturity model that allows risk management capacity weaknesses to be targeted quickly, without becoming constraining and/or invasive. As indicated within the report, the model is intended to assist projects/organizations to understand the maturity and possible shortcomings associated with risk management processes. As explained within the report, RMMM is largely based on the work of Hillson (1997) discussed earlier in the literature review.

As explained by RMRDPC (2002), the RMMM provides a framework that allows the implementation of a benchmark approach to risk management using four standard levels of maturity. The activities necessary to move to the next level are documented.

As indicated within the report provided by RMRDPC (2002), the RMM is based on the assumption that the maturity of risk management processes within projects/organizations can be categorized into groups that range from those who have no formal process to those in which risk management is fully integrated into all aspects of the project. As clearly emphasized within the report, the expectations of RMRDPC in designing the model were such that it was not expected that all projects/organizations would fit neatly into these categories. However, as explained within the report, the RMMM levels were defined sufficiently different to accommodate the diversity found in most projects/organizations. The four levels of the RMMM are found within the following table:

The Four Levels that identify the level of an organization’s Risk Management Maturity.
According to Artto and Hawk (1999), the current direction in project management is to promote learning and seek creative ways to conduct risk management. However, as explained by Hulett (2001), there are many projects and organizations that remain “risk-immature”. According to Hulett, some fail to learn much about risk management and thus do not practice it while others know something about the discipline but are inhibited in practicing it due to ingrained habits, prejudices and attitudes that prevent risk management. As well, others may understand it and attempt to establish the conditions necessary for applying it, only to discover that project/organizational cultural behaviors and barriers to risk management are difficult to overcome. Consequently, as explained by Hulett, project risk management is not as developed as are some of the more traditional project management methodologies.

In response to this problem, Hillson (1997) suggests several factors that further facilitate a risk maturity model in projects and organizations. As identified by Hillson, it is first critical that there is a commitment to risk awareness as well as to the efforts necessary to make a risk management program successful. Quite frequently, as discussed by Hulett (2001), organizations that are risk-immature also display an organizational culture that remains hostile to risk management. In such organizations, project risk management is perceived primarily as a competitive tool rather than one that can be utilized to achieve successful outcomes. Project plans are developed to meet the customer’s stated priorities even if meeting those priorities is not possible. In such environments, those supportive of risk management are often perceived as “selling out” and potentially jeopardizing the project. As explained by Hulett, changing the organizational culture remains one of the most difficult processes in making risk management successful.

There are four things you can do about a risk (Turbit, 2013). The strategies are:

- Avoid the risk. Do something to remove it. Use another supplier for example.
- Transfer the risk. Make someone else responsible. Perhaps a Vendor can be made responsible for a particularly risky part of the project.
- Mitigate the risk. Take actions to lessen the impact or chance of the risk occurring. If the risk relates to availability of resources, draw up an agreement and get sign-off for the resource to be available.
- Accept the risk. The risk might be so small the effort to do anything is not worth while.

Finally, as further suggested by Hulett (2001), risk maturity is truly reflected in projects/organizations that are willing to share working risk management approaches and practices. Through the visible exchange of ideas, project risk management as a discipline is provided the opportunity to grow in the development, improvement and application of more effective risk management skills, tools, concepts and practices.

CONCLUSIONS
In the words of a fellow Chicagoan, never let a good crisis go to waste. A unique convergence of circumstances makes this the perfect time to bring IT and business units
together under the flag of a risk-oriented approach to security. Economic stress and cutthroat competition on a global scale mean every dollar you spend on security had better matter. Plus, the money is there. Thirty-five percent of the 563 respondents to our InformationWeek Analytics IT Risk Management Survey say their companies' IT risk management programs will get more funding in 2011 than they did last year (Bataller (2011).

As was reflected in the preceding review, there is at present an extensive knowledge base on IS development. However, there is no evidence or documentation of efforts to study and investigate project risk management as it applies to IS development projects. This may be a consequence of the fact that both IS development and project risk management are relatively new and still emerging fields of study and practice. In spite of the sparseness of theoretical frameworks and discussions integrating the two disciplines as well as the lack of research investigating project risk management in IS development projects, the results of the literature review clearly provide documentation of the need for research in this area.

IS development projects can be expected to remain critical to complex modern organizations and, as the knowledge base and skills associated with IS development will certainly continue to expand at a rapid pace, it is critical to engage in efforts to study the nature of project risk management and the degree to which it occurs in IS development projects. The current information available on risk maturity in organizations appears to offer a strong basis for planning and developing research in this area. The risk maturity knowledge base could very well serve as a critical tool in aiding IS development project managers to establish effective and ongoing project risk management practices.

REFERENCES


BIOGRAPHY

Dr. Rell Snyder holds a DBA in Information Systems from Argosy University and is a Professor in the School of Engineering, Technology and Media at National University.