Journal of International Technology and Information Management

Volume 19 | Issue 1 Article 2

2010

A Framework for Identifying and Understanding Risks in Information Technology Projects

Jack T. Marchewka
Northern Illinois University

A Framework for Identifying and Understanding Risks in Information Technology Projects

Jack T. Marchewka
Northern Illinois University
U.S.A.

ABSTRACT

Managing the costs, complexity, and risks of IT projects continues to be a challenge for many organizations. Project risk management is becoming an important sub-discipline of software engineering, and focuses on identifying, analyzing, and developing strategies for responding to project risk efficiently and effectively. This paper presents an IT project risk identification framework to facilitate identifying and understanding various project risks as part of an overall project risk management process. The proposed framework should be of interest to IT practitioners during the creation of the project plan and over the course of a project so that appropriate and corrective actions can be taken as needed. Moreover, this risk identification framework should also be of interest to IT academics in terms of teaching project risk management or as a theoretical basis for future research. Taken together, this may help increase the likelihood of IT project success.

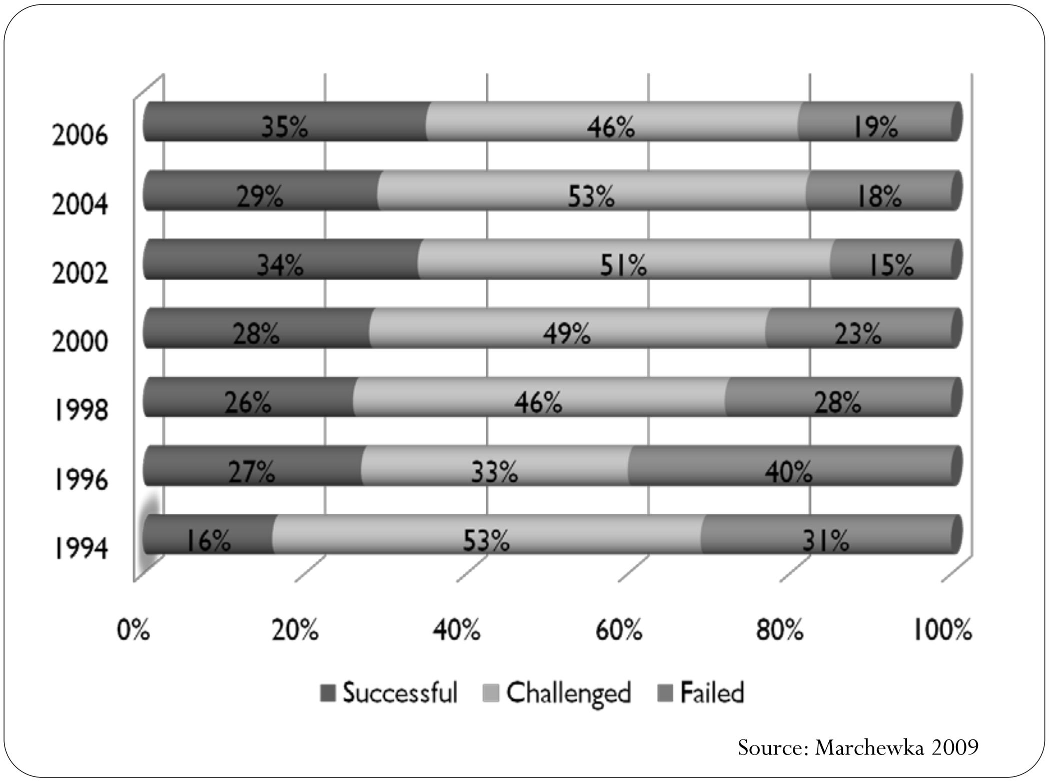
INTRODUCTION

Although information technology (IT) is becoming faster, more reliable, and less expensive, the costs, complexity, and risks of managing IT projects continues to be a challenge for many organizations. For example, a survey conducted by the Standish Group (1995) of 365 IT managers in 1994 drew attention to what many called the software crisis. The study was called CHAOS and reported that only 16 percent of the application development projects were successful in terms of being completed on time and within budget. Moreover, about 31 percent of the projects were canceled before completion, while 53 percent were completed but over budget, over schedule, and not meeting original specifications. The average cost overrun for a medium-size company surveyed was about 182 percent of the original estimate, while the average schedule overrun was about 202 percent. That is, the results of the survey suggest that a medium-size project estimated to cost about $1 million and take a year to develop actually cost about $1.8 million, took just over two years to complete, and only included about 65 percent of the envisioned features and functions. Many took this to mean that IT project management was in a state of crisis, especially since 48 percent of the IT managers surveyed believed that there were more failures at the time than five or ten years earlier.

However, the original CHAOS study published in 1994 was the first of several studies conducted every two years by the Standish Group. Figure 1 provides a summary of the CHAOS studies conducted from 1994 through 2006. Although, in general, it appears that the percentage of successful projects is increasing, a large percentage of challenged and unsuccessful projects suggests that there is ample opportunity for improving project performance. Therefore, having a well-defined, proactive risk management approach may contribute to the likelihood of project success.

ISSN: 1543-5962-Printed Copy ISSN: 1941-6679-On-line Copy

Figure 1: Summary of the CHAOS studies from 1994 to 2006.



Source: Marchewka 2009

In addition, a more recent study of 800 senior IT managers from the U.K., United States, France, Germany, India, Japan and Singapore conducted by Tata Consultancy Services (2007) reports dire results similar to the CHAOS studies:

- sixty-two percent of the IT projects failed to meet their schedules;
- forty-nine percent experienced budget overruns;
- forty-seven percent experienced higher than expected maintenance costs; and
- forty-one percent failed to deliver the expected business value and return on investment (ROI).

The purpose of this paper is to present an IT project risk identification framework that can be used to identify and understand various project risks before impending failure. The proposed risk identification framework should be of interest to IT practitioners during the creation of the project plan and over the course of a project so that appropriate and corrective actions can be taken as needed. Moreover, this risk identification framework should also be of interest to IT academics in terms of teaching project risk management or as a theoretical basis for guiding future research. Taken together, this may help increase the likelihood of IT project success.

IT PROJECT RISK MANAGEMENT

Project Risk and Project Risk Management

The Project Management Body of Knowledge (PMBOK®) Guide (2004) defines project risk as:

> *An uncertain event or condition that, if it occurs, has a positive or negative effect on the project objectives (238).*

The PMBOK® Guide provides an important starting point for understanding risk. First, project risk arises from uncertainty. This uncertainty comes from an attempt to predict the future based on estimates, assumptions, and limited information. Although project risk has a downside resulting from unexpected problems or threats, project risk management must also focus on positive events or opportunities. Therefore, it is important that project stakeholders understand what those events are and how they may impact the project beyond its objectives. It is also important that project stakeholders understand not only the nature of project risks but also how those risks interact and impact other aspects of the project throughout the life of a project.

Moreover, the PMBOK® Guide defines project risk management as:

> *…the processes concerned with conducting risk management planning, identification, analysis, responses, and monitoring and control of a project; most of these processes are updated throughout the project. The objectives of project risk management are to increase the probability and impact of positive events, and decrease the probability and impact of events adverse to the project (237).*

This PMBOK® Guide definition of risk management suggests that a systematic process is needed to manage effectively the risk of a project.

Project Planning and Managing Project Risk

A project plan is based on a number of estimates that reflect the project manager's understanding of the current situation, the information available, and the assumptions that must be made. The fact that one must estimate implies a degree of uncertainty in predicting the outcome of future events. Although no one can predict the future with 100 percent accuracy, having a solid foundation, in terms of processes, tools, and techniques, can increase the confidence in these estimates.

Unfortunately, things seldom go according to plan because the project must adapt to a dynamic environment. Project risk management is becoming an important sub-discipline of software engineering. It focuses on identifying, analyzing, and developing strategies for responding to project risk efficiently and effectively (Jones, 1994). It is important, however, to keep in mind that the goal of risk management is not to avoid risks at all costs, but to make well informed decisions as to what risks are worth taking and to respond to those risks in an appropriate manner (Choo, 2001).

Project risk management also provides an early warning system for impending problems that need to be addressed or resolved. Although risk has a certain negative connotation, project stakeholders should be vigilant in identifying opportunities. Although many associate uncertainty with threats, it is important to keep in mind that there is uncertainty when pursuing opportunities, as well.

Unfortunately, many projects do not follow a formal risk management approach (Jones, 1994). Because of their failure to plan for the unexpected, many organizations find themselves in a state of perpetual crisis characterized by an inability to make effective and timely decisions. Many people call this approach crisis management or fire fighting because the project stakeholders take a reactive approach or only address the project risks after they have become problems. Several common mistakes in managing project risk include:

- *Not understanding the benefits of risk management*—Often the project sponsor or client demands results. They may not care how the project team achieves its goal and objectives—just as long as it does. The project manager and project team may rely on aggressive risk taking with little understanding of the impact of their decisions (Lanza, 2001). Conversely, project risks may also be optimistically ignored when, in reality, these risks may become real and significant threats to the success of the project. Unfortunately, risks are often schedule delays, quality issues, and budget overruns just waiting to happen (Wideman, 1992).

- *Not providing adequate time for risk management*—Risk management and the ensuing processes should not be viewed as an add-on to the project planning process, but should be integrated throughout the project life cycle (Lanza, 2001). The best time to assess and plan for project risk, in fact, is at the earliest stages of the project when uncertainty for a project is the highest. Catastrophic problems or surprises may arise that require more resources to correct than would have been spent earlier avoiding them (Choo, 2001). It is better to reduce the likelihood of a risk or be capable of responding to a particular risk as soon as possible in order to limit the risk's impact on the project's schedule and budget.

- *Not identifying and assessing risk using a standardized approach*—Not having a standardized approach to risk management can overlook both threats and opportunities (Lanza, 2001). Consequently, more time and resources will be expended on problems that could have been avoided; opportunities will be missed; decisions will be made without complete understanding or information; the overall likelihood of success is reduced; and catastrophic problems or surprises may occur without advanced warning (Choo, 2001). Moreover, the project team may find itself in a perpetual crisis mode. Over time, crisis situations can have a detrimental effect on team morale and productivity.

LITERATURE REVIEW

The idea of managing IT project risk and risks associated with systems development has received attention in the IT literature in a variety of forms. First, several models for managing IT project risk have been proposed. More specifically, Barki, Rivard, and Talbot (2001) proposed an integrative model of software project risk management that combined contingency research in organizational theory with concepts of software risk management published in the information systems (IS) literature. The model hypothesized that project performance can be influenced by a combination of a project's risk exposure and how the project is managed in terms of a risk management profile.

In addition, Schmidt, Lyytinen, Keil, and Cule (2001) developed a list of common risk factors using a Delphi Study. They contend that the first step in managing IT project risk is the identification of risks so that appropriate counter measures can be taken. Subsequently, having a validated list of common risks could help a project manager understand the nature and types of risks they would most likely face.

In 2004, Tiwana and Keil developed a "One-Minute Risk Assessment Tool" for analyzing software development risks based on data collected from senior IT managers. This tool allows managers to differentiate between risks that fall within and outside of their sphere of influence. As a result, managers can conduct intuitive "what if" analysis to guide them in reducing software risks proactively since only risks that are underappreciated and unmanaged have the power to surprise.

In a study that looked at specific risk factors, Jitpaiboon and Kalaian (2005) used hierarchical linear modeling (HLM) to study top management as a risk factor for IT project success. Their findings suggest that IS projects are most likely to be successful when top management provides attention and sufficient resources to the project.

In addition, a model proposed by Wei and Peach (2006) assesses risks in global IT outsourcing relationships by identifying risk factors such as national infrastructure, organizational infrastructure, and the project environment. The model then attempts to logically link these risk factors so that relative weights can be measured and assessed.

More recently, Gemino, Reich, and Sauer (2008) propose and test a temporal model of information technology project performance (TMPP). They contend that it is important to separate risk factors as earlier (a priori) risk factors and later (emergent) risk factors. Moreover, a priori risk factors can have a direct influence on emergent risk factors. This study highlights the importance for active risk management that recognizes, plans for, and manages risk factors throughout the project life cycle.

However, a number of studies have focused on risk management in terms of specific areas of software development. For example, Nidel-Edwards and Steinke (2007) contend that missing important software requirements until later in the project is a critical risk in software development projects. Therefore, it is important to develop a thorough test plan that reduces the risk of discovering these important requirements before they can have an adverse impact on the project's schedule and budget.

Other studies have focused on risks associated with specific applications, technologies, or industries. For example, Wu, Hsieh, Shin, and Wu (2005) presented a methodology based on task-technology-fit theory to provide a systematic approach to alleviate the difficulty and complexity associated with identifying data and output misfits when evaluating off-the-shelf enterprise resource planning (ERP) packages. Similarly, Aloni, Dulmin, and Mininno (2007) collected and analyzed a number of key articles discussing and analyzing ERP implementations to compare different approaches with respect to risk management and highlight key risk factors and their impact on project success.

Finally, Adis (2007) provided a conceptual framework on risk modeling and described how it can be applied within the context of business process modeling within regulated industries. The framework was then applied to the U.S. Pharmaceutical industry, which is bound by stringent government mandates and risk adverse consumers.

AN IT PROJECT RISK IDENTIFICATION FRAMEWORK

Based upon the existing literature, it appears that the area of managing IT project risks has received some attention in a variety of areas and is a rich environment for further research. Studies, for example, have focused on the relationship between risk and project performance (Barki, Rivard, & Talbot, 2001; Jitpaiboon & Kalaian, 2005). Other studies have focused on specific software applications or technologies (Wu, Hsieh, Shin, & Wu, 2005; Aloini, Dulmin, & Mininno, 2007), industries (Adis, 2007), or the outsourcing relationship (Wei & Peach, 2006).

In addition, several important concepts should be included in an IT risk framework. More specifically, this would include a sphere of influence (Tiwana & Keil, 2004) and a time element that considers a priori and emerging risks (Gemino, Reich, & Sauer, 2008).

However, the PMI (2004) tends to view and treat project risk management as a set of processes that include risk identification, risk assessment, risk strategies, risk monitoring and controlling, and risk response. Approaches to risk identification tend to focus on techniques rather than specific tools that include brain storming, nominal group technique, the Delphi technique, or mind mapping. While Ishikawa or Fishbone diagrams could be considered a tool that can be adapted to risk identification, they tend to be more useful for analyzing a specific risk. Other tools such as checklists have limited value and appeal for three reasons: First, a checklist can lead to a false sense of confidence that all risks have been identified. Second, trying to identify every conceivable risk would be impossible or would make a checklist unwieldy and subsequently unusable. Or, on the other hand, a checklist has limited value if it is too broad or generic. And third, risk may be inherent to the context of a specific project.

Therefore, it appears there is a need for a tool or framework to help identify IT project risks that builds upon the existing literature and that can be used seamlessly within the process and techniques for identifying project risks.

The framework presented in this section provides a useful tool that can be used by project stakeholders to better identify and understand the myriad of risks that can impact an IT project. This framework can be used with such techniques as brain storming, nominal group technique, or the Delphi technique to provide an increased focus.

Risk identification provides an important first step and deals with identifying and creating a list of threats and opportunities that may impact the project's goal and/or objectives. Unfortunately, identifying and understanding the risks that will impact a project is not always a straightforward task. Many risks can affect a project in different ways and during different phases of the project life cycle. Therefore, the process and techniques used to identify risks must include a broad view of the project and attempt to understand a particular risk's cause and impact among the various project components.

The model illustrated in Figure 2 highlights several important components that are necessary for understanding and identifying risks and includes several important concepts from the existing literature. Using an analogy, the model may be thought of as an onion with several layers. The outer layer provides a temporal component that considers the notion or a priori or emerging risks (Gemino, Reich, & Sauer, 2008). Risk may have different impacts and probabilities during the different phases of the project. The next two layers take into account the idea specific risks can be underappreciated or have the power to surprise (Tiwana & Keil, 2004). Moving toward the center, the third layer focuses on the project infrastructure in terms of people, processes, technology, and so forth. The next layer focuses on the project objectives and includes scope, schedule, budget, and quality. Finally, the innermost layer reflects the value of the project to organization and is considered the core of not only the model, but the project itself. Each of these components is now discussed in more detail.

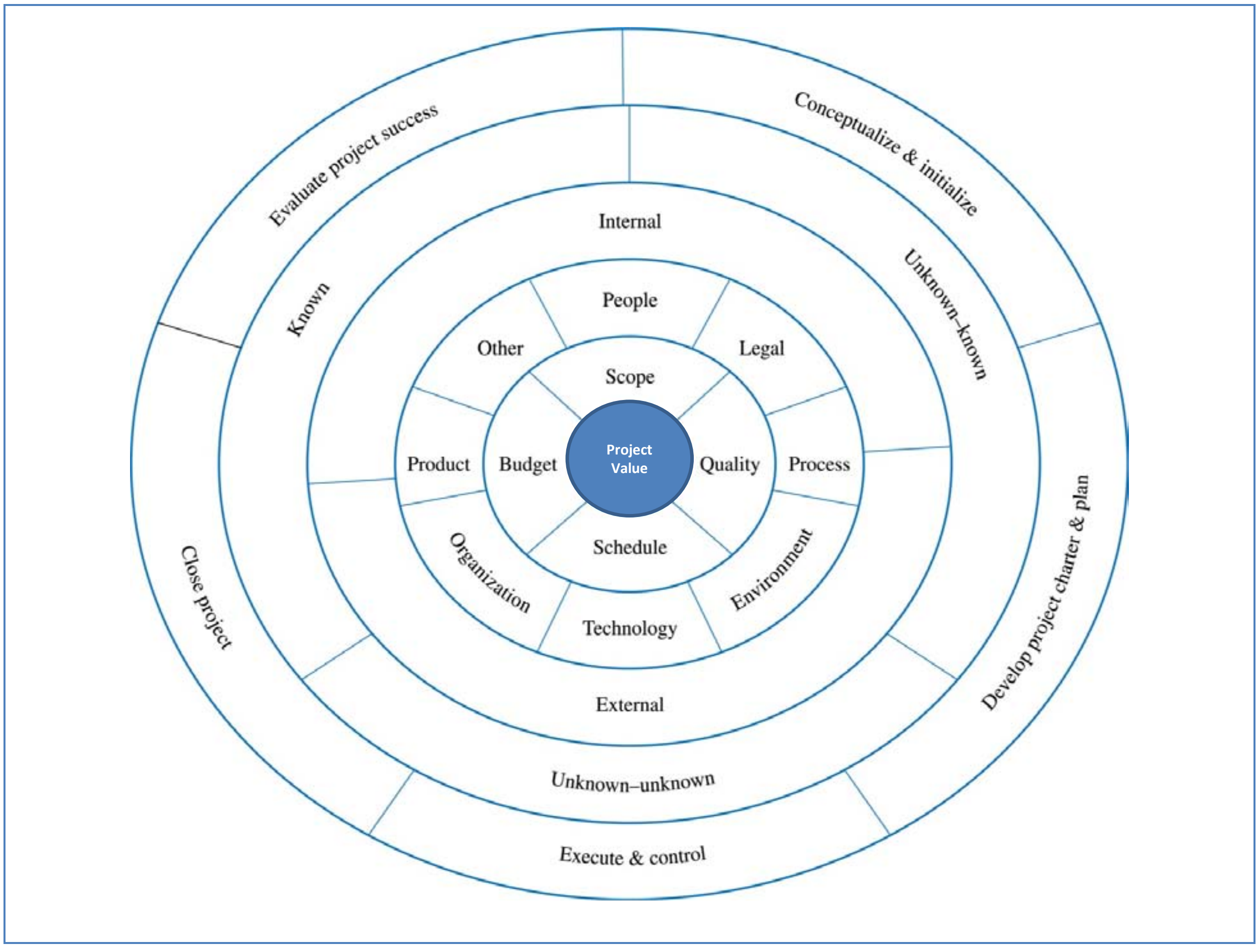
The project's value to the organization

Resources and time should not be devoted to a project unless they provide some kind of value to the organization. For example, an organization may invest in an IT project to penetrate new markets, provide customers with better products or services, to lower costs, or to increase operational effectiveness. A project's value that can be articulated and measured becomes a definition of project success (Marchewka, 2009). Therefore, a project's value is the core of the IT risk identification framework because risks, in terms of missed opportunities or adverse events, can subsequently lead to a challenged or failed a project. Risks that impact the project's value should be viewed as having the most impact. It is therefore important to identify risks as early as possible in order to mitigate a risk's probability and/or impact or to take advantage of any potential opportunities.

Project objectives

Moving from the core, the next layer of the framework focuses on the project objectives which are defined as scope, quality, schedule, and budget. While project objectives are important, they are not sufficient definitions of project success because success must be defined in terms of value to the organization. However, project objectives play a critical role in supporting the project's value to the organization because risks that impact project objectives can impede a project from delivering its anticipated value to the organization. For example, an organization may invest in an ERP project with the expectation that the post implementation of the system will reduce annual costs by $500,000. Moreover, the ERP project's budget may be estimated to be $1 million while the estimated schedule will be twelve months to implement. Most project stakeholders would probably agree that the project would not be a failure if implementation of the system took an extra day and went over budget by $1,000 because project success is defined in terms of expected cost savings. However, if various adverse events or risks impact the project's schedule and budget, overruns in terms of schedule and budget may overshadow the project's expected value. The project may become a failed project.

Figure 2: IT project risk identification framework.



The project infrastructure

Risks can arise as a result of the various people or stakeholders associated with a project, legal considerations, the processes (project and product), the project environment, the technology, the organization, the product, and a catchall category called other.

For example, one risk may be a key member of the project team leaving the project. The project schedule may be impacted if the skills, knowledge, and experience of that team member are difficult to replace in the relative short term. The time required to recruit a replacement, bring that person up-to-speed, and become a productive contributor to the team may consume valuable schedule, budget, or even compromise quality. The question then becomes, what impact will this have on the project's value? If the project's value may be impacted adversely, then the key project decision makers, such as the project manager or sponsor, may determine that paying a premium to recruit and hire a highly qualified replacement may be in the best interest of the project. On the other hand, a project manager or sponsor could identify the probability and impact of such a risk early on so that the risk of losing a key project team member could be avoided or mitigated.

Internal and external risks

The next layer focuses on whether the sources of risk are internal or external to the project. It is important to make this distinction because a project manager may be responsible and accountable for all project risks internal to the project. For example, if a project team member is not adequately trained to use a particular technology, then the project's objectives—scope, schedule, budget, and quality—may be impacted. In turn, this lack of training may inhibit the project from achieving its intended value. Once this project risk has been identified along with its impact, the project manager can avoid or mitigate the risk by sending this particular project team member to training or by assigning certain critical tasks to a more experienced or skillful team member. On the other hand, a project manager may not be responsible for external risks. For example, a project manager would not be responsible or accountable if the project were cancelled because the organization sponsoring the project went bankrupt.

The distinction between internal and external risks is not always clear. For example, even though a particular hardware or software vendor may be external to the project, the project manager may still be responsible if that vendor is unable to deliver required technology resources. If the project manager chose that particular vendor, he or she may responsible or accountable for that risk. In short, a project manager will (or should) have control over internal risks, but not necessarily external risks. That distinction does not mean the project manager can ignore external risks. These risks can have a significant impact on the project, as well as the project manager's career.

Known, known-unknown, and unknown-unknown risks

The fifth layer of the IT project risk identification framework includes three different types of risks: known risks, known-unknown risks, and unknown-unknown risks. Wideman (1992) defines known risks as events that are going to occur. In short, these events are like death and taxes—they will happen and there is no uncertainty about it. On the other hand, known-unknowns are identifiable uncertainty. For example, a project manager may need to hire a database administrator. This would the "known" part of the risk. The "unknown" component would be the negotiated salary and subsequent prorated cost of using that resource needed as an estimate in the project plan. Unfortunately, the project manager may have to make assumptions when planning the project's budget before this resource is acquired and the cost known.

Unknown-unknown risks, on the other hand, are residual risks or events that are difficult to anticipate. For example, hazardous weather, political instability, or economic recessions are a challenge to predict. Unknown-unknown risks are reminders that there may be a few risks remaining even after we think we have identified them all. In general, these are the risks are easier to identify after they occur.

Project life cycle phases

The outer layer provides a time element in terms of the project life cycle (PLC). These phases include *Conceptualize and Initialize, Develop Project Charter and Plan, Execute and Control, Close Project, and Evaluate Project Success* and can incorporate various phases of the systems development life cycle (SDLC) as well. A time element may be useful for identifying the likelihood of when a particular risk may occur. For example, a risk of not accurately identifying the requirements of a system may arise during the *Execute and Control* phase of the project when analysis and design activities are scheduled. Risks associated with this activity will therefore have the highest probability of occurring and the most impact during this time period of the project. Moreover, the probability and impact of this risk will be different or nonexistent during other phases of the project. As a result, the project manager can understand this particular risk's source, in terms of the project environment, and its impact on the project's objectives and value and therefore plan accordingly.

APPLYING THE IT PROJECT RISK IDENTIFICATION FRAMEWORK

An example may be useful to better understand how to apply the IT project risk identification framework in Figure 2. A consulting firm has been hired by a client to develop a data warehouse that will include business intelligence to identify and better serve its more loyal customers. The project is still in the early stages, with the baseline project plan and charter almost finalized. Unfortunately, the client has been hit hard by an economic recession.

The client is now challenged financially and must cut costs to survive. Not surprisingly, a number of the client's managers may suggest that the data warehouse project be cancelled. However, due to the expected value the project can bring to this organization, it is decided that the product's scope will be cut in half in order to create two projects—one that will provide minimum functionality and another project that will add the remaining features and functions once the company becomes more financially stable. The project's new scope will be reduced in order to reduce the budget and schedule as well. The risk faced by the project stakeholders could be viewed as:

- A threat that occurred in the *Develop Project Charter and Project* plan phase. It was an unknown-unknown risk because it was identified after it occurred and, therefore, caught the project team off guard.

- It was an external risk, and the project manager and project team should not be held responsible for the economic downturn experienced by the client.

- The sources of risk to the project include environment (economic), organizational (the client) and people (it could be argued that management was responsible for this problematic event).

- The impact on the project was significant because it would affect the project's scope, schedule, and budget. Since the consulting firm was able to renegotiate the contract based on a trimmed scope, we can assume that quality would not be an issue. But if the client's management insisted on maintaining the original scope, schedule, and budget, chances are good that quality would become an issue, especially if, for example, the scheduled testing time had to be shortened in order to meet the scheduled deadline.

- It is likely that the project's value to the organization would change as well because the project team would not complete the scope as originally planned. This would in turn require a revised scope, schedule, and budget for the project.

This example shows how a risk can be understood after it occurs. The framework can also be used to proactively identify IT project risks. For example, a project team could begin with the project phases defined in the outer core of the framework. Using the project's work breakdown structure (WBS) and the individual work packages, the team could identify the risks for each of the work packages under the various project phases. Again, it is important that both threats and opportunities be identified.

These risks could be classified as either known risks or known-unknown risks. The category of unknown-unknown risks should serve as a reminder to keep asking the question, What other threats or opportunities have we not thought about? Hopefully, the project team will do a more thorough job of identifying risks early in the project and reduce the likelihood of being surprised later.

The risks identified by the team can then be categorized as external or internal to the project. The internal risks are the direct responsibility of the project manager or team, while external risks may be outside their control. Regardless, both external and internal risks must be monitored and responses should be formulated.

The next step involves identifying the various sources of risk. Instead of trying to neatly categorize a particular risk, it may be more useful to understand how the sources of risk are interrelated with each other. In addition, it may be a situation where precise definitions get in the way of progress. Instead of arguing or worrying about the exact source of a particular risk, it is more important the stakeholders understand the complex nature of a risk. Each risk-source category may mean different things to different stakeholders. Depending on the project, the stakeholders should be free to develop their own definitions and interpretations for each risk source category. They should also feel free to add categories, as needed.

After identifying the nature and characteristics of a particular risk, the project team can assess how a particular risk will impact the project. At this point, the team should focus on the project objectives that would be impacted if a particular risk occurred and, in turn, whether the project's value to the organization would be impacted. Later on, these risks can be assessed to determine how the objectives will be impacted.

The example shows how, working from the outside and then inward toward the center of the model, risks can be identified using the IT project risk identification framework. This procedure works well as a first pass and when using the project plan or WBS as a source of input. Many threats and opportunities may, however, be overlooked when relying only on the WBS.

In addition, the project team could start with the inner core of the IT project risk identification framework and work outward. For example, the project team could identify how the project's value may be affected in terms of threats or opportunities that affect the project's scope, schedule, budget, or quality. Working away from the center, the team could identify possible sources of risk and then categorize whether the risk is internal or external, known, known-unknown, or unknown-unknown (i.e., did we miss something?), and when during the project life cycle this particular risk might occur.

CONCLUSION

Risk is an inherent component of IT projects because the project plan is based on a number of estimates that reflect a project manager's understanding of the current situation, the information available, and the assumptions that must be made. But, events seldom go according to plan, so the project must adapt to an ever-changing environment. An inability to predict the future with 100 percent accuracy coupled with a dynamic environment create degrees of uncertainty or risk that must be addressed and managed throughout the project life cycle.

Although risk implies a negative connotation, project stakeholders must be vigilant in identifying opportunities presented by risk. The Project Management Body of Knowledge (*PMBOK® Guide*) points out that project risk management provides a systematic process for identifying, analyzing, and responding to project risks. A project risk management approach should focus on maximizing the probability and impacts of positive events while minimizing the probability and impacts of negative events. This may lead to a higher likelihood of project success.

The framework presented in the paper builds upon the existing literature and takes a more holistic view of risk. For project managers, this provides a starting point that should be incorporated into a process for project risk management. Future directions for research could include case studies or empirical studies that could include the testing of hypotheses. More specifically, this could include the temporal components of particular risks and the impact of risks on the project's objectives and overall value.

REFERENCES

Adis, W. (2007). A risk modeling framework for the pharmaceutical industry. *Communications of the IIMA*, 7(1), 1-10.

Aloini, D., Dulmin, R. & Mininno, V., (2007). Risk management in ERP project introduction: Review of the literature. *Information & Management*, 44(6), 547-567.

Barki, H., Rivard, S., & Talbot, J. (2001). An integrative contingency model of software project risk management. *Journal of Management Information Systems.* 17(4), 37-70.

Choo, G. (2001). It's A Risky Business. http://www.gantthead.com/content/articles/18271.cfml

Gemino, A., Reich, B. H., & Sauer, C., (2008). A temporal model of information technology project performance. *Journal of Management Information Systems*, 24(3). 9-44.

Jitpaiboon, T., & Kalaian, S. A. (2005). Analyzing the effect of top management support on information system (IS) performance across organizations and industries using hierarchical linear modeling. *Journal of Information Technology and Information Management,* 14(2), 131-144.

Jones, T. C. (1994). Assessment and Control of Software Risks. Upper Saddle River, NJ: Yourdon Press/Prentice Hall.

Lanza, R. B. (2001). Reviewing a Project Risk Management System. www.auditsoftware.net/infoarchive/articles/projmgmt/files/riskmgmt.htm

Marchewka, J. T., (2009). *Information Technology Project Management: Providing Measurable Organizational Value.* Third Edition. John Wiley & Sons. New York, NY.

Nindel-Edwards, J. & Steinke, G. (2007). The development of a thorough test plan in the analysis phase leading to more successful software development projects. *Journal of Information Technology and Information Management,* 16(1), 65-72.

Project Management Institute (PMI). (2004). *A Guide to the Project Management Body of Knowledge (PMBOK Guide).* Newtown Square, PA: PMI Publishing.

Schmidt, R., Lyytinen, K., Keil, M., & Cule, P., (2001) Identifying software project risks: An International Delphi study. *Journal of Management Information Systems,* 17(4), 5-36.

Standish Group. (1995). *CHAOS.* West Yarmouth, MA: The Standish Group.

Tata. (2007). http://www.tcs.com/news_events/press_releases/Pages/ITprojectunderperformanceacceptedasthenormbyglobalbusinessmanagementresearchreveals.aspx

Tiwana, A. & Keil, M. (2004). The one-minute risk assessment tool. *Communications of the ACM*, 47(11), 73-77.

Wei, J. & Peach, B. (2006). Development of a risk assessment model for global information technology outsourcing. *Journal of Information Technology and Information Management*, 15(4), 35-50.

Wideman, R. M. (1992). *Project and Program Risk Management: A Guide to Managing Project Risks and Opportunities*. Newtown Square, PA: Project Management Institute.

Wu, J. H., Hsieh, C., Shin, S. S., & Wu, C. C., (2005). A methodology for evaluating data and output misfits in commercial off-the-shelf ERP systems. *Journal of Information Technology and Information Management*, 14(4), 27-74.