Risk Management for IT Projects

Introduction

There are a variety of standards associated with risk management including PMI's Project Management Body of Knowledge (PMBOK), Australia-New Zealand ANZ-4360, International Standards Organization (ISO) ISO 31000 Risk Management -- Guidelines on Principles and Implementation of Risk Management, ISO/IEC 16085 Systems and software engineering – Life cycle processes – Risk Management, National Institute of Standards and Technology (NIST) 800-30 Risk Management Guide for Information Technology Systems, Factor Analysis of Information Risk (FAIR), Institute of Electrical and Electronics Engineers (IEEE) 1540, and many others. PMBOK, ANZ-4360, and ISO/IEC 16085 focus primarily on project risk management whereas NIST 800-30, ISO 31000, and FAIR have a much broader scope and focus primarily on organizational or Enterprise risk management. Fundamentally, all of these standards have five basic components in common; risk management planning, risk identification, risk analysis, risk treatment, and risk monitoring.

The focus of this whitepaper is specifically project risk management and the primary references are the PMBOK, ANZ-4360, and ISO/IEC 16085. This white paper will focus on common challenges associated with project risk management, present a practical approach to risk management based on PMBOK, ANZ-4360, and ISO/IEC 16085. A brief discussion about how an enterprise can derive maximum value from project risk management is also included.

IT Project Risk Defined

Webster's defines risk as "exposure to the chance of injury or loss; a hazard or dangerous chance".

ANZ-4360 defines risk as "the chance of something happening that will have an impact on objectives."

PMBOK defines project risk as "an uncertain event or condition that, if it occurs, has a positive or negative effect on at least one project objective, such as time, cost, scope or quality."

By any definition, risk is something rather nebulous that, if it happens, will be undesirable. Because of the nebulous nature of risk many people find it difficult to effectively manage the risk. This white paper presents a number of techniques that will help Project Managers and Risk Managers make project risks less nebulous so that they can be effectively managed.

Risk Management Challenges

When discussing risk management with Project Managers I encounter four recurring challenges that I consider significant impediments to effective project risk management; improperly defined risks, risks not properly quantified, ineffective mitigating strategies, and lack of documentation about the effectiveness of the mitigating strategy.

The most common risk management challenge is that risks are not properly identified. Project Managers and team members will frequently identify conditions, symptoms, events, and / or opinions that are indications that a risk exists but, they do not decompose the risk to the point that the actual risk is identified. In looking at risk logs, I will see literally dozens of risks that are symptoms or indications that a risk is present but the actual risk never makes it to the log. If the risk is not properly identified it becomes nearly impossible to mitigate. Project teams spend countless hours mitigating various symptoms while the actual risk goes unscathed. Project risks should be identified in terms of schedule, budget, quality, or mission accomplishment.

The second risk management challenge is that risks are not properly quantified. I see risks logs that list the impact as "major", "significant", "substantial", etc. In order to effectively mitigate a risk its impact to the project must be objectively quantified. For example, three-week schedule delay, $50,000 budget overrun, 500 hours of rework, etc.

The third risk management challenge is preparing an effective treatment plan. I often see risk logs containing dozens or hundreds of risks with each risk containing a single mitigating action. A risk with a single mitigating action is one indication that the project risk has not been properly identified. Further analysis often reveals that the same mitigating action is assigned to a variety of risks; another indication that the true risk has not yet been properly identified. More often than not, a risk will require multiple actions to be effectively mitigated. Mitigating strategies also provide significant value at the Enterprise level which will be discussed in more detail later in this whitepaper.

Finally, the fourth risk management challenge is a lack of documentation regarding the effectiveness of the mitigating strategy. Not documenting the effectiveness of the mitigating strategy may not necessarily impact the current project but, it will certainly affect later projects. The effectiveness of mitigating strategies should be documented and push up into the PMO, Enterprise, etc.

Risk Management Process

An effective project risk management process consists of nine components; six discrete process steps and three activities. The six process steps are; establish the context, identify risks, quantify risk impact, prioritize risks, treat risks, and monitor risk strategy. There are three activities that transcend the entire risk management process; oversight to ensure compliance, develop risk models, and feedback loop. The PMBOK, ANZ-4360, and ISO/IEC 16085 include the same nine components although they may be ordered and grouped differently.

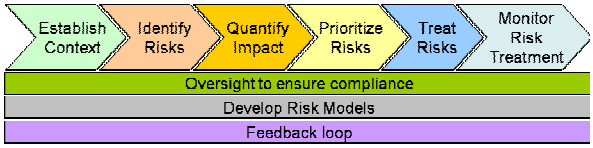

Figure 1 - Risk Management Process

Some may argue that the sequence is less important that the actual process. However, I have found that the following sequence is the most effective as it maximizes the risk management effort by focusing on high impact risks and reduces the amount of effort wasted on low impact risks.

Establish the Context

Organizations frequently broaden the scope of project risk management to include areas outside of the project team's direct control. Requiring project teams to manage risks well outside of their project boundary not only causes confusion and wasted effort but also indicates the need for a Program or Project Management Office (PMO). PMO's are much more capable and effective than a project team in mitigating risks across an organization. The context of project risk management should be confined to the project's budget, schedule, quality, and mission accomplishment.

Identify Risks

One of the greatest challenges to effective project risk management is the proper identification of risks. Project risks frequently have a variety of symptoms, conditions, events, etc. that indicate the presence of a risk. Project teams will often times identify these risk indicators as the risk while, the real risk goes undocumented and slips by under the radar. The real danger of identifying risk indicators instead of the true risk is that the true risk goes undocumented and undocumented risks cannot be managed.

Improper identification of risks can lead to extremely large risk logs filled with a combination of risks, risk indicators, issues, etc. Risk logs of this nature quickly become unmanageable because of their size. A single risk may have dozens of symptoms or conditions each of which requires significant effort to document, develop treatment plans for, and report the status. While the project team is spending countless hours attempting to manage risk indicators, the real risk is incurred which not only causes schedule delays, budget overruns, poor quality, etc., but also leads the project team to lose confidence in their ability to effectively manage risk. In addition to risk indicators, risk logs frequently contain issues which further compound the problem and lead to even more confusion. A risk log containing dozens or hundreds of entries can quickly become daunting and very intimidating to the project team that questions their ability to effectively manage risks.

A hurricane is one example of an event that is often identified as a project risk. A hurricane will significantly impact a project team working in a hurricane prone area but, even though the effects of the hurricane can be minimized, the hurricane itself cannot be managed by the project team. The key point here is to recognize the difference between conditions or events that cannot be managed (e.g. asteroid hitting the earth, hurricanes, etc.) by a project team and risks that can be managed. One question to ask is; how much time and effort should the project team spend attempting to manage these types of conditions or events? Another event that I frequently see logged as a risk in the Public Sector is "regulatory change". Once again, "regulatory change" is an event that cannot be managed by the project team; however, the schedule and budget risks associated with unexpected requirements changes (associated with regulatory changes) can be managed and will be addressed in the next section.

I contend that risks must be defined in terms of schedule impact, budget impact, quality impact, or ability to accomplish the mission. If schedule impact can be effectively managed then it doesn't matter what condition or event impacts the schedule (i.e. hurricane, network outage, personnel turnover, etc.). There are five basic questions that can be asked to help identify project risks:

1. Is there a schedule impact?
2. Is there a budget impact?
3. Is there an impact to quality?
4. Is there an impact to our ability to accomplish the mission?
5. Can impact be objectively quantified?

If the answers to questions 1, 2, 3, or 4 and 5 are "yes" then there is a very good chance that the risk has been properly identified.

Quantify Risk Impact

In order to effectively manage a risk, its impact to the project must be objectively quantified. For example, three-week schedule delay, $50,000 budget overrun, 500 hours of rework, etc. "Significant delays", "reduced quality", "Substantial cost overrun", etc. are extremely problematic when defining risk primarily because "substantial cost overrun" to one person could mean hundreds of dollars whereas "substantial cost overrun" to someone else could mean tens of thousands of dollars. Quantifiable impact is also crucial when monitoring risks since it makes little sense to spend $100K to manage a risk that has an impact of $50K.

Project teams often struggle with quantifying risk impact. Quantifying risk impact is further compounded by the fact that many "risks" are not truly project risks and cannot be managed by the project team; the hurricane scenario previously mentioned is one example.

It is possible that a risk can affect multiple aspects of the project; a schedule delay for

example could also impact the budget. In order to effectively manage the risk it is important to understand the driver(s) behind the project. If time to market is more important then the risk should be defined and managed as a schedule risk whereas if budget is more important then the risk should be defined and managed as a budget risk. The project sponsor will most likely have to make the decision as to whether time to market or budget is most important.

It is possible to manage both a schedule and a budget risk (e.g. project team works unpaid overtime) but often at the risk of quality. The schedule, budget, quality triangle is outside the scope of this whitepaper however, there are countless articles and books available (see links in the Further Reading section below).

Consider the following scenario based on the "regulatory change" event noted in the previous section:

- There is a pending regulatory change that will require unplanned modifications to the project
- If the regulatory change goes into effect then additional scope will need to be added to the project.

Once it has been determined that a risk exists (by asking the five key questions), the next step is to determine the potential impact. In this case, there will definitely be an impact to the schedule since increased scope will require either additional resources or redeploying existing resources; in either case, the schedule must be modified. In order to determine schedule impact the scope must be analyzed to some degree and the effort to implement the required changes must be estimated. Let us assume that the scope will require approximately 500 hours of effort to implement. "500 hours" is a quantifiable metric that can be used to prioritize and manage the risk. Based on the project driver(s), the 500 hour estimate can be expressed in terms of schedule impact or budget impact. If budget is the driver, then a part of the treatment plan could be to redeploy existing resources which would result in a schedule delay but would keep the budget on track. If schedule is the driver then a part of the treatment plan could be to add additional resources to the project which would result in cost overrun but keep the original schedule. The schedule impact can be explicitly defined simply by multiplying the number of additional resources required by the duration (e.g. 3 resources redeployed * 4 weeks = 12 week schedule impact). The budget impact can be explicitly defined by multiplying the cost of additional resources times the duration (e.g. 3 additional resource (@ $5,000 / week cost) * 4 weeks = $75,000 budget impact).

In this particular scenario, the best approach could be to issue a change order and remove some existing scope in order to accommodate the new regulatory mandated changes. There are other actions that could be implemented but these serve to illustrate the point.

Prioritize Risks

After risks have been properly identified and quantified, the next step is to prioritize the risks. Some may argue that developing a risk treatment plan should be the next step in the sequence but I contend that it is more effective to prioritize risks first so that risk management effort can be focused on the high impact risks. It makes little sense to spend time and effort to develop risk treatment plans for low impact risks that will result in schedule impacts of hours or days while the project is on the verge of incurring a risk that will result in schedule delays of weeks or months. Prioritizing risks will yield the most value to the project team by focusing the effort on the high impact risks. Risks should be prioritized based on impact to the project followed by probability of occurrence. There are countless risk prioritization schemes ranging from very simple high/low schemes to extremely complex schemes such as Monte

Carlo simulation. I prefer a simple 3-tier scheme of low, medium, and high which is often referred to as the 9-box model (depicted in Figure 2). The 9-box model calls for prioritizing risks with high impact / high probability to be managed first, followed by risks with high impact / medium probability and so on. In keeping with the objective quantification of risks, parameters must be established for high, medium, and low. The impact parameters require a quantified value for each context; Table 1 illustrates one example:

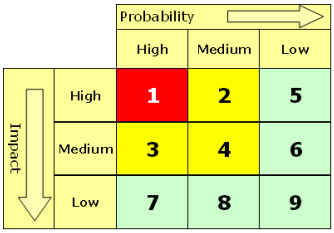

Figure 2 - 9-Box Model

Context	Impact	Parameter
Schedule	High	> 6 Weeks
	Medium	2 – 5 Weeks
	Low	< 2 Weeks
Budget	High	> $100,000
	Medium	$50,000 - $99,999
	Low	< $50,000
Quality	High	> 1,000 Hrs Rework
	Medium	500 – 999 Hrs Rework
	Low	< 500 Hrs Rework
Mission	High	Failure chance >65%
	Medium	Failure chance 35%-65%
	Low	Failure chance < 35%

Table 1 - Quantifiable Impact Parameters

The parameters for probability can be the same for all contexts (e.g. schedule, budget, quality, mission accomplishment). I suggest starting with a baseline of >80% for high, 50% - 79% for medium and <50% for low. Over time these parameters can be adjusted based on actual performance in a particular environment.

Treat Risks

The first step in the risk treatment process is to select one of the four industry accepted risk treatment strategies; Avoid, Transfer, Mitigate, and Accept.

Avoidance is a risk strategy where the project plan is modified to completely eliminate the risk. For example: A risk has been identified with a new software feature that is scheduled to be part of the next software release. The risk is estimated to impact the schedule by more than two months. To avoid the risk, the software feature associated with the risk can be de-scope and removed from the next release.

Transfer is a risk strategy where the risk is transferred to another party. The most common example of risk transfer is buying insurance. Subcontracting is another example of risk transfer.

Mitigate is a risk strategy where a risk treatment plan is prepared. A risk treatment plan is based on a mitigation strategy or series of actions that will reduce the impact of the risk to some degree. Risk treatment is one area where I prefer to utilize ISO/IEC 16085 or ANZ-4360. Both ISO/IEC 16085 and ANZ-4360 have very comprehensive sections related to risk treatment. ANZ-4360 contains excellent detailed information about creating treatment plans along with a variety of scenarios to help illustrate the process. The ANZ-4360 approach to risk treatment plans is very comprehensive and includes:

- Proposed actions
- Resource requirements
- Responsibilities
- Timing
- Performance measures
- Reporting and monitoring requirements

ANZ-4360 includes two components that are notably absent in both the PMBOK and ISO/IEC 16085; “timing” and “performance measures”. The “timing” and “performance

measures" can be combined to establish a trigger point for initiating different actions of the risk treatment plan. Having said that, I prefer the ISO/IEC 16085 treatment plans overall because it is very comprehensive and addresses a number of areas that are not covered in either the PMBOK or ANZ-4360 (e.g. resource allocation, control measures, environment requirements, treatment change procedures). These missing components are extremely important and contribute to the development of risk models which are covered later in this white paper. ANZ-4360 utilizes the concept of "triggers" which, when combined with the ISO/IEC 16085 treatment plan, provides an extremely comprehensive and highly effective risk treatment plan.

To help illustrate the use of triggers, consider the following scenario:

- A key deliverable on the critical path has been subcontracted to an organization that has a reputation for late delivery.
- Based on the Treatment Plan in Figure 3, a trigger point has been established and two actions have been defined that are tied to the trigger point (1 – Identify alternate supplier(s) and 2 – Engage alternate supplier(s)).

Risk	Resources Requirements	Proposed Action	Timing	Performance measures	Reporting and Monitoring
Schedule delay > 2 weeks due to late delivery by subcontractor	Contract Specialist (CS) Project Manager (PM)	Develop performance based contract with supplier(s)	Prior to project start		N/A
		Establish weekly milestones	Prior to project start		N/A
		Conduct weekly progress reviews	Weekly - ongoing		Weekly Progress Report
		Identify alternate supplier(s)	30 days prior to the trigger point		Project Schedule
		Establish a trigger point for engaging alternate supplier(s)	Prior to project start		Project Schedule
		Engage alternate supplier(s)	• Earned value is < 90% at the trigger point OR • Earned value is < 75% at weekly progress review	Earned value	In accordance w/Communication Plan

Figure 3 - Risk Treatment Plan

The key point here is that specific decision(s) or trigger points are explicitly defined along with specific actions that must be undertaken at that point. Explicitly defining actions and the "trigger" to initiate the action reduces the likelihood that actions will slip and it also makes the treatment plan repeatable. Explicit actions and trigger points are in stark contrast to soft trigger points and subjective criteria (e.g. "engage the alternate supplier when you are sure that the supplier will be late")

Acceptance is the final risk management strategy. There are two categories of risk acceptance; passive acceptance and active acceptance. Passive acceptance essentially means that the project is simply going to accept the risk and deal with the risks as they arise (aka issues). Active acceptance involves establishing a contingency reserve of time, money, and resources to deal with risks as they arise. Acceptance is a reasonable risk management strategy in cases where the cost of mitigating a risk is more than the impact of the risk. Passive acceptance relegates the project or organization to incur nearly all potential risks. Active acceptance is a common strategy when dealing with many unknowns (e.g. space travel), leading edge development, etc.

Important Note: Passive acceptance is the default risk management strategy for any project or organization that does not have a formal and effective risk management process.

Monitor Risk Treatment

There are two categories of risk monitoring; tactical and strategic.

Tactical monitoring occurs day to day and is typically conducted by the project team. Tactical monitoring should be conducted on a daily basis and must take performance measures, trigger points, and actual performance into account. The purpose of the tactical day to day monitoring is to evaluate whether the risk treatment plan is effectively mitigating the risk(s). The tactical monitoring should evaluate actual progress against the performance measures in the treatment plan and trigger points should be monitored on a daily basis. It would not be prudent to spend

$100K mitigating a risk that will result in $50K loss so, it is very important to measure the cost and effort associated with risk treatments and not blindly execute the risk treatment plan.

Strategic monitoring is conducted as part of management reviews, during internal or external audits, and at the end of projects. Strategic monitoring is forward looking and focuses on long-term process improvement. An important aspect of strategic monitoring is post-project risk analysis. Risk analysis evaluates the results of risk treatment plans and their associated performance measures looking for patterns and anomalies which become inputs to risk models.

Risk Models

One of the most important outcomes of the risk analysis process is the development of risk models. A risk model is a risk strategy or risk treatment plan that has been proven to be effective for a recurring risk. A risk model will contain proven mitigating strategies, resources, proposed actions, triggers, performance measures, and reporting information. Additionally, the risk model will include risk strategies and/or treatments that were applied but were found to be ineffective. Risk models can be developed based on a variety of factors (e.g. methodology, project size, team size, technology stack). The real value of the risk model is that effective actions and strategies are validated and ineffective actions are documented so that subsequent project teams can focus on proven treatment plans.

Oversight to ensure process compliance

The project risk management process is not complex but, executing the process can be very difficult. In order for project risk management to be effective, the process must be enforced at both the tactical and strategic level. Effective oversight of the tactical risk management process can be provided by a combination of Quality Assurance reviews and Management reviews. Oversight of the strategic risk management process requires fairly rigorous process compliance and is most effective if an organization supports formal Quality Management procedures. Without adequate oversight, the effectiveness of organizational risk management can quickly deteriorate due in large part to the challenging nature of project risk management.

Feedback Loop

An active feedback loop is one area where an organization can derive a tremendous amount of value from project risk management. An active feedback loop is characterized by processes that "push" information throughout the organization as risk models and lessons learned are develop or modified. Actively disseminating information allows project teams to leverage enhanced risk models, lessons learned, etc. on a near real-time basis. Wiki or other collaboration software are excellent tools for providing active feedback to project teams, especially distributed teams.

Conclusion

Unfortunately, there is no single, definitive source for risk management processes, tools, techniques, etc. However, highly effective and comprehensive risk management process can be constructed using components of the PMBOK, ANZ-4360, and ISO/IEC 16085. The PMBOK contains a good overview of project risk management and includes what should be considered the basic foundation for the strategic aspects of organizational risk management (e.g. risk models, risk management oversight, quantitative risk analysis). ISO/IEC 16085 has a very comprehensive risk management plan, an excellent approach to risk treatment, and also includes more detailed governance topics (e.g. risk management policies, risk management

roles and responsibilities, risk thresholds). Even though ANZ-4360 has been superseded by ISO/IEC 16085 it does contains more detailed processes along with a number of tools and techniques that can be used to augment ISO/IEC 16085. Additionally, ANZ-4360 utilizes the concept of triggers which simplifies the decision making process in times of crisis and yields repeatable risk treatment plans.

Finally, keep in mind that risk management is not a complex process. The key to effective risk management is to follow a defined, disciplined approach and focus on objective measures for identifying, quantifying, and prioritizing risks.

Keys to effective project risk management
Implement a defined process
Properly identify project risks
Quantify risk impact using objective measures
Prioritize risks based on probability and impact
Develop a mitigating strategy
Monitor mitigating strategies
Develop reusable risk models
Provide oversight to ensure compliance
Implement an active feedback loop

Table 2 - Risk Management at a Glance

Bio

Mr. Mayo is a PMI certified Project Management Professional (PMP) and PMI certified Risk Management Professional (RMP). Mr. Mayo's career has spanned more than 27 years and includes 13 years of hands-on software development and 16 years of Project and Program Management. Mr. Mayo has spent 17 of the past 27 years as a consultant for a number of companies including CSC and Keane. Mr. Mayo has conducted more than 60 IT project assessments with emphasis on PMBOK compliant project and risk management processes. Mr. Mayo holds a BS/IT degree from the University of Phoenix. Career highlights include:

Program Manager for #7 of InfoWorld's Top 100 IT Projects of 2006. Developed PMO governance, the collaboration workspace, and Executive level dashboards to divest a large International conglomerate. The PMO was responsible for cloning 112 Corporate Applications for four separate operating companies, and renegotiating 1,300 telecom, IT service and license contracts without impacting the day to day operations of any one of the operating companies.

Program Manager for the Air Force Supply Modernization. Utilized the Rational Unified Process (RUP) and the Evolutionary Process for Integrating COTS (EPIC) to deliver new capability that dramatically improved the efficiency of the Air Force supply chain resulting in a ROI calculated at 6:1 in the first 12 months alone.

Mr. Mayo can be contacted via e-mail at jwmayo@north-country.net

Further Reading

Project Triangle
http://en.wikipedia.org/wiki/Project_triangle

Respect the Iron Triangle
http://www.ittoday.info/Articles/IronTriangle.htm

Discussion of Risk Management
http://www.cs.adfa.edu.au/~ejl/Portal/Systems%20planning/SP%20pages/Risk_paper.htm

Development of Risk Management Defense Extensions to the PMI Project Management Body of Knowledge
http://www.dau.mil/pubs/arq/2003arq/Spring2003/ConrowSP3.pdf

References

ANZ-4360 Risk Management Guidelines
http://www.saiglobal.com/shop/Script/Details.asp?DocN=AS564557616854

PMBOK Guide, Fourth Edition
http://www.pmi.org/Marketplace/Pages/default.aspx?Category=PMBOKBooks

ISO/IEC 16085 Systems and software engineering – Life cycle processes – Risk Management
http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40723

Appendix A – Risk Treatment Plan

The following treatment plan example is based on ANZ-4360:

Risk	Resources Requirements	Proposed Action	Timing	Performance measures	Reporting and Monitoring
Schedule delay > 2 weeks due to late delivery by supplier	Contract Specialist (CS) Project Manager (PM)	Develop performance based contract with supplier(s)	Prior to project start		N/A
		Establish weekly milestones	Prior to project start		N/A
		Conduct weekly progress reviews	Weekly - ongoing		Weekly Progress Report
		Identify alternate supplier(s)	30 days prior to the trigger point		Project Schedule
		Establish a trigger point for engaging alternate supplier(s)	Prior to project start		Project Schedule
		Engage alternate supplier(s)	• Earned value is < 90% at the trigger point OR • Earned value is < 75% at weekly progress review	Earned value	In accordance with Communication Plan

Appendix B – Risk Treatment Plan Outline

The following outline is based on ISO/IEC 16085

1. Overview
   1.1. Date of Issue and Status
   1.2. Issuing Authority
   1.3. Updates
2. Scope
3. Reference Documents
4. Glossary
5. Planned Risk Treatment Activities and Tasks
6. Treatment Schedule
7. Treatment Resources and their Allocation
8. Responsibilities and Authority
9. Treatment Control Measures
10. Treatment Cost
11. Interfaces Among Parties Involved
12. Environment / Infrastructure
13. Risk Treatment Plan Change Procedures and History

