IBM Global Business Services
White Paper

Insurance

Risk assessment and management process in projects

"To be successful, the organization should be committed to address risk management proactively and consistently throughout the project. A conscious choice must be made at all levels of the organization to actively identify and pursue effective risk management during the life of the project. Risk exists the moment a project is conceived. Moving forward on a project without a proactive focus on risk management increases the impact that a realized risk can have on a project and can potentially lead to project failure."[1] *(p 276)*

Introduction — Why read this?

How often have you heard the phrase “We don’t know what we don’t know”? You would hear this pronouncement probably daily in the consulting industry. To paraphrase a recent insurance commercial, “What you don’t know can hurt you” highlights the important role risk management plays in today’s business environments and in particular in project management. At the heart of the risk management process lies the understanding of the risk’s potential impact and its probability of occurrence. It is through this knowledge that the best risk strategy and response can be developed and aligned with the organization’s own sense of risk tolerance or “appetite.”

The risk assessment and management process in a project must be well-thought out and tailored to the organization.[2 (p 3)] However, regardless of the organization’s sophistication, certain universal principles still apply. The process must be robust and thorough but balanced for ease of use; in other words, the process can not be a bureaucratic nightmare. The process must be positioned to quickly identify risks, and facilitate and communicate rapid and effective courses of action. Thus, from individual projects to billion-dollar businesses, having an effective and efficient risk management process is not only a wise business decision but also an obligation to a company’s stakeholders.

What will I learn by reading this white paper?

This paper explains the importance of understanding risks and provides insights on how to manage risks inherent to a project In many organizations, overall project management is planned and managed by a project management office (PMO). Our focus is how to develop, implement and maintain a project risk management process as part of such a PMO. Finally, there are case study examples of how a project risk management process was created, implemented and maintained for two US companies.

This paper draws primarily from individual consultants’ experiences who also were guided by risk management principles from the Project Management Institute (PMI) “A Guide to the Project Management Body of Knowledge (PMBOK Guide),” Fourth Edition. For the purposes of this paper, a “project” can represent the wide range of initiatives managed by the PMO, from individual projects to programs and portfolios.

Business problem — What is it?

Many project managers do not understand their risk environment, and worse still many **may think** they understand their risk environment. They may have a risk management process in place, but it may be flawed and thus provides a false sense of confidence that project risk is understood and being addressed. A project manager may have identified a risk but may have woefully underestimated the risk and have potentially placed his organization in danger and exposed to loss.

How well do project managers understand the risk? Inherently it is a “bad thing” (there are good risks, but that is beyond the scope of this discussion), but some risks are worse than others and must be so judged. A collision to your car is a bad thing and may certainly justify auto collision coverage. However, a collision to a paid-for 20-year-old clunker is a little different than that to a new Corvette that you happen to own with the bank. It’s the same thing in project management; a potential risk to a project’s schedule, budget or scope must be judged in the context of other projects, the overall program and to the sponsoring entity.

Thus in a project management context you have to understand the risk environment, identify, assess and prioritize the risks in that environment and plan what you actually do about those risks. The last point is particularly important, because you need to accurately weigh the benefits of such risk mitigation activities to the resources required for those activities.[2 (p 90)]

Develop a risk management process—How to address

An important first step is gaining senior management approval and support for a project risk management process. The commitment of a senior-level sponsor is critical for the resources requirements, organization process change and implementation, and ongoing support and maintenance. This initiative will be tested in that corporate stakeholders and project management staff will of course support the intent of project risk management, but full commitment may be a considerable stretch.

Compliance may exist, but a truly effective program requires commitment, and to that end having a senior-level "champion" is essential. In many organizations, senior sponsorship may come from the chief risk officer, chief audit officer or even the board of directors. In many situations, a risk management shortcoming has been identified through an audit or senior leadership initiative. However, committed senior leadership support cannot be assumed. Senior leadership support and direction must be publically announced and documented. Initially, a project risk management charter to establish, staff and implement this function must be developed, publicized and formally launched.

Once established, the new project risk management function must identify the criteria to evaluate and prioritize risks. In a PMO context, potential criteria could be cost, time or scope.[1] (p 291-2) Other criteria could also involve corporate social responsibility and ethical considerations or be closely aligned with organizational values and reputational risk.[2] (p 96) Ideally, they should have been identified at a high level as part of the project risk management charter. It is essential to identify the categories and then establish tolerances for evaluating a risk in those categories.

A simple example is project budgets. Yes, cost control is essential, but what tolerances are involved? Are you necessarily concerned about a budget over variance of 1 percent, especially midway through a one-year project? On the surface, it's not a huge variance but a variance in what context? If that 1 percent represents USD10 million, then maybe a problem exists, and variance definitions are required.

The example below lists categories of budget and schedule risks further delineated with a numeric scale that assigns a value to levels of category variance. Example for budget and schedule:

Numeric value →	**1**	**2**	**3**	**4**	**5**
Category ↓					
Budget variance	Plus or minus 1% variance to baseline	Plus or minus >1–5% variance	Plus or minus >5–10% variance	Plus or minus >10–20% variance	Plus or minus >20% variance
Schedule	Minimal impact to schedule	Two-week project delay 8	Four-week project delay	One-to two-week delay to overall project/ program critical path	Greater than two-week delay to overall project/ program critical path

The previous example documents the risk's potential impact to the project. The next factor in risk assessment is the probability that the risk may actually occur. Generally, the probability factors must be developed with ease of use in mind. Common practices have used a 1–5 scale broken out by 20 percent gradients.[3] (p 12-13)

For example:

1	2	3	4	5
20% or less	21–40%	41–60%	61–80%	81% or better

This breakout facilitates ease of use and self-application by staff analyzing the risk's probability. The breakout allows a few simple, intuitive questions to guide the assessment:

- Is there an even chance this risk may occur? Assign a 3 (41–60%).
- If not an even chance, is the probability an extreme? Assign a 1 (20% or less) or a 5 (81% or better) as appropriate.
- If not an even or an extreme chance, where does the probability trend to-ward? Assign a 4 (61–80%) if trending toward happening and a 2 (21–40%) if trending toward not happening.

In conjunction with the impact criteria, you now have the basis for a multiplicative matrix that combines the impact scores (1–5) with the probability scores (1–5). In their simplest forms, you have:

Impact →	1	2	3	4	5
Probability ↓					
5	5	10	15	20	25 (5x5)
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1 (1x1)	2	3	4	5

This Probability/Impact table provides a way to calculate a composite score that can equate to a risk priority assignment[1] (p 292)—a priority that can then dictate how a risk is managed, reported and governed. An example is using a color code to equate to a high risk (red), a medium risk (yellow) and a low risk (green). In the same table:

Impact →	1	2	3	4	5
Probability ↓					
5	5	10	15	20	25 (5x5)
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1 (1x1)	2	3	4	5

This Probability/Impact table serves as an indicator of risk tolerance or appetite and can be shifted as directed by senior leadership. In designating the risk distribution, some considerations include:

- Do the extremes of 1x5 (low probability x high impact) necessarily equate to a 5x1 (high probability x low impact)? Consider Russian roulette; is that not a low probability (1 in 6 chances) but a catastrophic impact? Conversely, is a 1x5 risk commensurate? For example, is hitting yourself in the head with a hammer a high probability versus, relatively speaking, a lesser impact of a nearcertain headache?
- There are no right or wrong determinations but a gut feeling on what is truly a high-priority risk. Such determinations are not made in isolation but must be a collaborative effort.
- The collaborative effort must be guided by what resources are available to monitor and manage identified risks. If there are considerable resources and bandwidth, the above matrix could be all red, meaning the company tracks all risks as high risks. Conversely, limited resources may dictate that only the most catastrophic risks be actively tracked and managed.
- The risk matrix or appetite is not set or permanent but can evolve in time to reflect risk experience, understanding and risk management process maturity.

Risk priorities of high, medium and low are descriptive terms but can only provide value if they represent necessary actions or protocols. As an example, for a high-priority designated risk, what action is required? Specifically:

- What are the time requirements and limits for mitigating this risk?
- What risk strategies are allowed? Can a high-priority risk be simply accepted versus mitigated, transferred or avoided?[1 (p 303)]
- What are the reporting frequencies and content?
- What is the oversight level? Who can authorize accepting a risk?

Risk priority levels must be defined and similarly instituted with corresponding risk management approaches. Sample approaches may include

Risk priority levels

Category of approach ↓	High priority	Medium priority	Low priority
Approve risk assignment	Vice president of risk management	Project manager	Originator
Approve mitigation due dates	Close or mitigate within two weeks	Close or mitigate within four weeks	Close or mitigate within six weeks
Approve mitigation plans	Required within one week of risk identification	Required within two weeks of risk identification	Optional
Approve ownership assignment	Project manager	Assigned by project manager	Assigned by project manager

Approach design must weigh the available resources to the required attention the organization deems appropriate. Approach categories could include status reporting, meetings to be recommended and governance requirements. The robustness of the approach is a factor of the resources allocated.

It is through approach development and adherence to approach requirements that the true power and value of the project risk management process can be realized. Unless there is clearly defined accountability and status reporting follow-up, risk management may very well fall victim to shifting corporate priorities. Earlier in this discussion we noted the importance of corporate support and the need for senior sponsorship and commitment. Such leadership is now critically important in maintaining focus and adherence to project risk management requirements and procedures. As appropriate, project risk reporting should be a regular agenda item at the project or program steering committee or in a PMO's own status meeting with senior leadership. If a project is being briefed, then its risks must be included. In these forums the project manager must be held accountable for managing and resolving project risks.

Implement the risk management process—How to start

To this point it is assumed that resources are assigned and you are actually developing the initial framework of the previously mentioned project risk processes, definitions and approaches. Ideally, this development was initiated by the critically important senior leadership sponsorship. At this point, implementing the envisioned project risk management process must start. Implementation requires change and as such, consideration and planning of major change drivers. Sample areas to consider:

- Processes and procedures—as previously discussed and as developed
- Organizational structures—How will the PMO be supported—through dedicated resources or part-time allocations?
- Skill set requirements—For the assigned resources, what will be the required prerequisite skill sets? What training can be used? How will people be hired?
- Reward mechanisms—What systems will be used to promote positive adherence to project risk management procedures, processes and requirements? How will noncompliance be addressed?
- Systems requirements—What system requirements must exist or be procured? How will risk artifacts in the public domain be tracked and managed

Important support mechanisms and activities must be planned and implemented to ensure that these change drivers succeed. Communication is central to gain stakeholder awareness, compliance and support for project risk management. This comprehensive communication strategy must be developed and executed by appropriate staff. Other support activities, including staff training, recruitment, position documentation and reward systems, must be developed and implemented in the corporate organization.

Once requirements and components are understood and defined, a comprehensive implementation plan must be created and executed. Options exist on who should have oversight and implementation responsibilities—the PMO or a centralized corporate risk management entity. Project Risk Management is a principle knowledge area under the PMBOK discipline[1] (p 273) and thus a strong argument for assignment to the PMO. However, project risk guidelines and requirements must be consistent with the corporatewide risk requirements.

Corporate risk tolerances and levels must be centrally developed and communicated to the PMO. These tolerances are then integrated and executed by the PMO in its program and project risk management processes. However, best practices also offer that the PMO involve corporate risk management in the project risk management development. It's through this joint familiarization between corporate and the PMO that an effective understanding of project management practices can be understood and the corporatewide risk requirements can be best translated to the PMO level.

Maintain the risk management process—How to maintain

Once established, the PMO project risk management requirements must be reinforced and maintained in light of an initial pushback and potential loss of interest or momentum. Initial pushback may be encountered, because project risk management takes resources and time, which are scarce commodities of any project manager and organization. Further, the goals of effective project management are simply not compliance but exceptional awareness of the risk environment, and to put in place effective and efficient risk strategies and mitigation plans is essential to project success. Senior managers must embrace this concept and reinforce their expectations through regular communication and actions.

Once implemented, it is hoped that the program's value would maintain interest and support. But sadly, that is not the reality, and key performance measures are necessary. Two measurement categories are suggested: process maturity measures and process compliance measures. The former indicates how well the overall risk management process is doing, and the latter measures individual compliance with risk management requirements.

Risk management process maturity can be assessed using various measures tracked over time, such as:

- Percentage of correct impact assessments for documented risks
- Percentage of risks with documented mitigation plans
- Average assigned quality marks for documented mitigation plans
- Average duration time to close or mitigate a risk
- Percentage of risks overdue or exceeding due dates
- Distributions of high-, medium- and low-priority risks

At an individual risk level, the same measures can be used, such as:

- Impact assessment consistent with published risk impact criteria
- Mitigation plan present and quality mark assigned
- Mitigation plan up to date and maintained
- Milestone dates accurate and not past due
- Duration times (risk initiated to risk closure) within standards

Accountability and visibility are important parts to overall project and risk management viability and value. In a perfect world, a committed risk management program will provide a substantial return in risk mitigation effectiveness and project efficiency. Minimal compliance will at least provide visibility to the risk environment and facilitate required actions.

Leadership visibility is demonstrated by management review and time dedicated at appropriate steering committees, PMO status meetings or board meetings. If a project is reviewed, there should be agenda space for reviewing risks and their mitigation plans. Bandwidth may always be an issue and thus the importance of accurate risk impact analysis and prioritization. If anything, high-priority risks must have regular oversight and review by senior leadership.

Leadership review means nothing if project risk management inaction or ineptitude is not addressed. Project managers are responsible for risks in their projects. They must be held accountable at appropriate venues or meetings if a risk is 1) poorly assessed and analyzed and 2) poorly addressed or mitigated. At a minimum, a project manager must accurately assess a risk, document an action plan and show progress to resolve.

Expectations must be made in project status meetings and communications that risks and their mitigation status will be reviewed and accountability affirmed. Project manager job descriptions must include risk management responsibilities and designate skill requirements. Annual—or more often as required—performance plans should include separate sections on risk management performance as well as other factors associated with project management performance. Substandard risk management performance must be reflected in the annual performance plan; standards also serve as midyear benchmarks to provide corrective action and direction. Adherence to these standards provides the teeth to risk management processes. Leadership's regular review of project risk management performance is an ongoing reinforcement of these standards and measures.

There is also a strategic impact to the project management and corporate risk management practices within the organization. Inconsistent or marginal leadership support endangers, through association, other management processes within the PMO and the greater corporate organization. Risk management by its nature and content is a critical service and activity; senior leadership indifference or perceived lack of support marginalizes this and other project management processes.

Improve the risk management process—How to adjust

Like any process, there must be adjustments consistent with a continuous improvement mindset essential in any healthy organization. In project risk management, you must determine whether the expected value is being realized. You can make this determination through the previously reviewed process maturity measures and through a review of high-priority risks.

Questions to be asked include:

- Has there been improvement in the process maturity measures?
- Have projects benefited through risk identification, and were the mitigation plans effective in resolving the risk?
- Were projects kept on schedule, scope or budget?
- For risks that actually occurred, was there a previously identified risk? Did that risk's mitigation plan help reduce the incident's impact?
- For risks that did occur, was the impact assessment accurate for what actually occurred?
- Did the risk appetite, as depicted in the Probability/Impact table, accurately reflect the distribution of risks in the PMO? Did such a prioritization effectively distribute management resources to the most appropriate risks?
- What feedback or lessons learned were gained? Were they distributed to the organization for continuous improvement?

PMO leadership and other senior leaders should jointly review such results and evaluate corrective action. Periodic reviews and monitoring of these questions will dictate the frequency of more formal reviews and actions. Minimally, an annual review should be conducted and perhaps in concert with the performance reviews of PMO leadership.

Case studies

Case study: A small life insurance company in the United States implemented project risk management processes as part of its comprehensive PMO approach.

A small life insurance company, although limited in resources, understood the ramifications of risks in various complex and ongoing projects. A strong proponent of communication, the company developed concise definitions of risk impact assessments and implemented transparent management procedures to oversee the risk mitigation activities. Although the project portfolio was relatively small, the potential for strategic implications was present and realistic. PMO leaders defined and implemented a governance structure that brought high-priority, organizationwide risks to their immediate attention and just as important, required a plan to address. A critical contributing success factor was the emphasis of a corporate culture where potential risks could be identified, discussed, escalated and acted on in a nonpunitive manner. The company realized the following benefits:

- Clear expectations—Project managers worked and thrived in an environment where they had clear definitions of what constituted project risk. As dictated by the risk potential, they were given the authority to mitigate risks at their level.
- Effective senior leadership—Risks identified under these definitions were easily escalated to more appropriate levels. Senior leadership was therefore effectively and efficiently focused on the most important risks.
- Visibility and expectations of action—High-priority risks were regularly presented at steering committee meetings as was an action plan defined by milestones, tangible outcomes and accountability by name.

The PMO established steering committee governance and discipline. Project status was presented, but the focus was deviations to a project's plan, not activities going according to plan. There are other considerations that impact a project's schedule, budget or scope, but effectively identifying risk is essential to preproject contingency planning and, in the event of risk actualization, resolving risk fallout. Senior leadership's understanding of this process and genuine support was instrumental in a valid and value-added risk management program.

Case study: A large financial services company establishes a comprehensive risk management and escalation program to support a large multiyear IT initiative.

This large financial services company was implementing a vast initiative to create a wide range of new services, systems and integrated capabilities. A wide assortment of project management processes was required, including a robust project risk management process. Risk management was co-managed by a team also responsible for issue management and escalation. Although two separate disciplines, they were tightly linked by project impact, potential risk or actual issue, and were executed at the project level by the same project staff. The impact assessments used were identical in each program, and their use dictated a prioritization and escalation that was basically the same. The company realized the following benefits from this massive initiative:

- All participants had a common language and understanding on what constituted a risk or issue to their project, programs and phases of the initiative. The external linking of a risk's impact to its program—and thus a critical-path effect outside the project—was essential. Risk impacts were a crucial component of dependency management.
- Definition of the initiative's risk tolerance was facilitated by adjusting the risk impact definitions. All risks were not high, nor could senior management see and act on them all. In such a massive effort, clear but adjustable definitions could determine the flow of crucial risks to senior managers. In circumstances where truly high-priority risks were overwhelming, management bandwidths and further staffing needs could be adjusted.
- Risks and their priority were easily documented and categorized in collaborative databases, which facilitated individual tracking and consolidated initiativewide performance tracking. Risk priority served as a key classification and tracking value. Data tags and links to these risks allowed efficient senior leadership review and insights without inordinate searches for the truly critical risks. Risk classifications also dictated certain business rules and process time standards that facilitated updates and required actions.

Without the discipline and definition of risk and issue impacts, centralized PMO oversight would be overwhelmed by the sheer volume of data from hundreds of projects. Risk prioritization facilitated the efficient categorization of this data and further linked these insights to other processes, most notably dependency, change and requirements management. Clear definition and justification of a risk's priority was essential in such a complex and vast initiative.

Conclusion

The risk of not knowing your risks is substantial, but once understood it provides a context by which you deal with those risks. A project manager must evaluate their environment, identify the risks and then decide what to do. Senior leadership must provide the definitions for assessing the risk environment and the criteria by which to categorize that risk. Proper classification is essential for providing clear criteria for expected action—action that mitigates a risk at a local level or, as priority dictates, at a higher level.

Clear and timely communication of what to do is half the challenge. Senior managers must dedicate the time and effort to address understanding and assisting in risk mitigation at their level. These high-level or strategic risks have impact beyond a project, essentially endangering the organization's long-term objectives. Such risks must be governed, seen and escalated with appropriate action plans with demonstrated risk mitigation progress.

A key challenge is to foster and reinforce an environment where it is acceptable and professional to escalate risks and to initiate a proactive action plan. Anything else will severely hinder the honest flow of communication to senior leadership. Senior leadership's risk awareness and a genuine motivation to remove obstacles and maintain a project's momentum is essential for organizational success.

About the authors

Patricia Brooks is a Senior Managing Consultant in the IBM Global Business Services Insurance Practice. She has 16 years of experience within the insurance industry as a consultant, team leader and manager. She specializes in Agile Methodology, risk and issue management and business process improvement.

William Couch is a Managing Consultant with the IBM Global Business Services Insurance Practice. He has over 25 years experience in the insurance industry and in management consulting. His areas of expertise is in project management, process improvement, strategy development and strategic change. He holds the PMP, CPCU and FLMI designations.

Lee Tate is a Senior Manager in the IBM Global Business Services Insurance practice. He has 30 years of extensive commercial and personal lines insurance and business process experience blending both business and technical perspectives. He has performed in many roles in client engagements, from business analyst to road map development, from technical project management to implementation leadership for core financial systems.

References

1 “A Guide to the Project Management Body of Knowledge (PMBOK Guide),” Fourth Edition, Project Management Institute 2008

2 “Managing Risks in Projects,” Dr. David Hillson, 2009

3 “Guidelines for Risk Management,” NASA, Independent Verification & Validation Program, March 25, 2009

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
September 2013

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

♻ Please Recycle