PRM Best Practice: The PCNet Project[1]

1.1 Background

In 2002, the first-tier diversified resource company, Metal Resources Co., headquartered in Austin, Texas, announced a cash offer for the Winnipeg-based metals company, RBD, Inc. The offer was recommended by the RBD board to its shareholders and then swiftly executed. The combined companies formed the second largest mining and resources company in the world. In 2004, Metal Resources Co. had activities in 28 countries, with $29 billion in sales, 40,000 employees, and leadership positions in aluminum, nickel, copper, uranium, gold, carbon steel metals, diamonds, manganese, and various specialty metals used in steel production.

The acquisition execution placed heavy emphasis on synergies, that is, on gross annual cost savings. Five top-level integration areas were put in place to capture the savings: IT infrastructure, HR systems and processes, financial systems and processes, operational integration, and organizational integration. The total synergy target amounted to $1.9 billion in annual gross operating cost savings.

One of the important merger activities was a consolidation of the IT systems of the two companies, a huge undertaking involving 900 IT employees throughout the combined company. Not only had the IT integration achieved its own target of $210 million in savings, but it also critically enabled the other merger areas by providing a transparent, integrated, and reliable application platform. Max Schmeling, the enterprise CIO, was responsible for executing the IT integration.

A pre-integration team planned the integration project in detail over a period of nine months, up to October 2002. The team started from an overall target ("get $210 million in annual savings by consolidating the IT structure") and successively broke this target down to more and more detailed tasks. Within each consolidation area, large projects were defined, then subprojects, and then detailed tasks that could be assigned. In total, 110 projects were to be executed in parallel by project managers and subproject managers, supported by a central project office. The projects would have to be carefully coordinated, as some of them served as enablers for others, and all competed for the same scarce staff time.

In September 2002, Max Schmeling pulled his direct reports and operating company CIOs into one room (about a dozen people). He presented them with the work breakdown structure that the planning team had produced. He said, "Nobody leaves this room before every one of the 110 savings opportunities has a name on it." The first outcome of this two-day marathon meeting was a project structure that clearly assigned project accountabilities, as well as a corporate sponsor for each project, to help them drive change through the organization. The key projects within the IT integration were "General" (mainframe decommissioning, Unix integration, and office consolidation at the various sites of the previous companies), knowledge management (including the consolidation of portals, intranets, yellow pages, instant messaging, collaboration tools, and publishing), the ERP program (moving to an enterprisewide SAP installation encompassing HR systems and financial reporting across both companies), the Web applications center, IT strategy (which was to connect the IT changes to head counts and reengineered processes, and strategic IT sourcing), and the PCNet project, on which our project risk management (PRM) example focuses.

The last piece, not producing bankable savings but critical nonetheless, was the "Time Zero" project: The IT systems were changed while

simultaneously running the business. Critical systems, such as e-mails, global address lists, help desks, and all business applications (but not, for example, cross-unit calendar lookup), had to work on day one. Without this minimal functionality, the business damage would have been too great, and resistance would have prevented a successful execution of the migration.

The second outcome of the marathon meeting was a "Gantt Chart from Hell," which filled an entire wall. This was a preliminary plan showing how the 110 projects would be sequenced, and when they would reach their critical milestones and, ultimately, completion. In addition to encompassing a large number of tasks, the planning job was made even harder because the 110 projects had to be coordinated with the other synergy projects and with the activities of the operating companies, who were responsible for carrying out numerous activities.

1.1.1 The PCNet Project

The PCNet project encompassed four network infrastructure migration areas (see Figure 1.1): (1) worldwide standard desktop environment, mostly the exchange of the 40,000 companywide desktops, standardizing on Windows XP desktops (HP) and laptops (IBM); (2) a global communications network, consolidating the corporate network (which had previously been centered on the bottlenecks in California and Texas) around six hubs, with added bandwidth to the rest of the network and further internal redundancy; (3) a standard network server infrastructure using Windows 2000, with a greatly reduced number of network routers; and (4) an enterprise security and directory system, going from multiple directories, security systems, and firewalls down to one each. Multiple directories caused headaches when, for example, executives were reassigned and stopped receiving their e-mails until the IT staff had located the directory in which they had been filed.

The business case called for a total savings net present value (NPV) of $115 million, with a project budget of $149 million. This was based on direct savings from infrastructure costs alone, but the project was the key enabler of the whole merger, not just the IT integration. It enabled additional savings, including cutting 130 different applications in the Finance area alone, and it later made the transition to an enterprisewide ERP system much faster and smoother.

The network integration included the reconciliation of outsourcing decisions that had been made differently in the previous companies. For example, Metal Resources had outsourced mainframe, telecom, and the help desk to EDS, while RBD had outsourced the server environment and the help desk to IBM. To move fast, IT management decided to move the entire package to EDS (the provider who already had the bigger share) and to take some server services back in-house.

Project objective: Integrate Metal Resources' desktop, network, and server structure, and directory and security services.

- 40,000 desktops migrated to global standard (31,000 from Metal Resources and 9,000 from RBD), investment $89 million, NPV $83 million
- 900 network routers consolidated. Investment $29 million, NPV –$2 million
- Network structure with 500 servers centralized to three hubs with standard servers. Investment $13 million, NPV $20 million
- 10 directories and 7 security systems consolidated to one standard each, Investment $15 million, NPV $14 million

(NPV Assumptions: 4-year savings NPV (after investment), 10% discount rate, tax, and depreciation included)

Figure 1.1 The PCNet project

The PCNet project organization included a project management office, a group for implementation and operations, and a planning group comprising several analysts who compiled business cases and risk analyses, and maintained the tracking tools. Embedded in the master plan for IT integration, the PCNet planning group developed and maintained its own plan and milestones (Figure 1.2). Much of the actual work (such as physically installing routers in basements and desktops in offices) was performed by local staff in the operating companies; the central project organization coordinated, standardized, oversaw time plans, and centrally sourced the standardized components.

1.2 Risk Identification

Risk identification is concerned with recognizing, at the outset, the factors that may make the project plan obsolete or suboptimal. Thus, risk identification is an important part of project planning. It represents a thorough homework exercise that allows the project organization to be prepared when adverse events strike, offering ready-made (rough-cut) solutions, based on which a team can respond quickly.

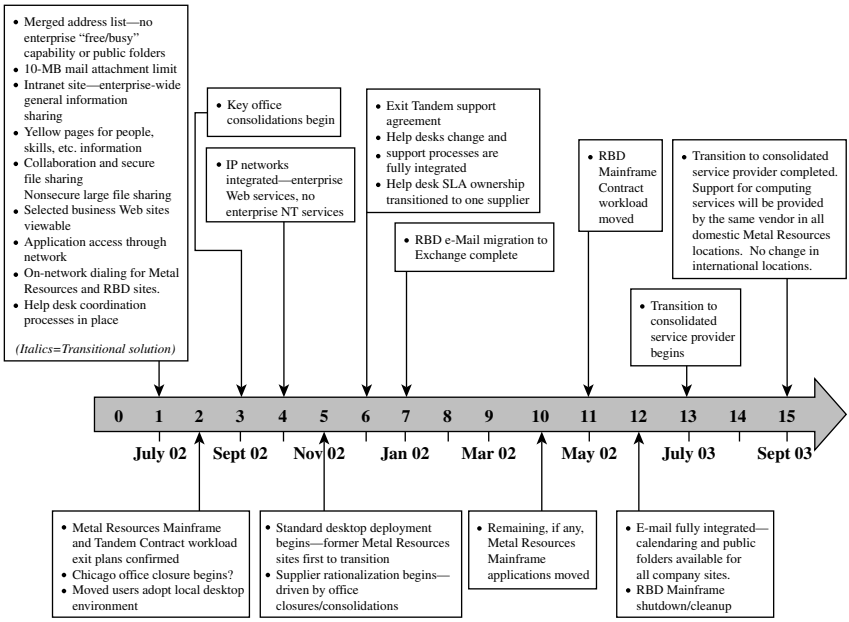


Figure 1.2 The PCNet project key milestones

In the PCNet project, risk planning was a formal part of all project plans. The main risk areas were seen as Operating Company acceptance (they had to perform, and pay for, a lot of the detailed implementation work, and they resented the distraction from their pressing priorities); "staying focused," meaning dealing with too many activities with the same scarce resources; security breaches during the transition; and a change in business climate that would threaten the availability of funds to complete the merger.

This aggregate list rested on many lower-level risk identification efforts, one of which is shown in Figure 1.3, focusing on HR and personnel retention risks. The list showed where the risk's impact would lie (e.g., in achieving synergies); whether the impact was financial, on the schedule, or on solution quality; and how high the impact would be financially. Finally, the list estimated the risk probability and indicated the impacted parties and the "owner," i.e., the party responsible for responding to the risk.

The lower-level risk lists (such as the one illustrated in Figure 1.3) were produced by the project management office in collaboration with the operating divisions that performed much of the work. The project management office produced a draft list based on experience from previous projects, and the execution teams added risks, based on the detailed tasks, systematically asking what could possibly go wrong. In other words, the risk lists combined knowledge and experience with project-specific planning.

Risk Description	Risk Category	Risk Type	Risk Probab.	Risk Impact	Parties impacted	Risk Owner	Status			Comments
Describe the Risk	Synergy; Day one; Bus. local; Bus. global	Time (T) Financial (F) Quality (Q)	H = >80% M = betw L = < 20%	H = > $5m M = betw L = < $1m	Project Team Impacted by Risk O = Owner I = Impacted	Person responsible for monitoring and reporting	Mitigated?	Open/Closed?	Assigned?	General Notes
			%	$ (one yr.)						
ATTRITION of technology talent could jeopardize exploration, and IT operations and transition	**All**	T F Q	M	H	I: ALL (operations, exploration, technology, finance, IT/systems, corporate, HR integration, procurement) O: IT/systems	CTO tecnology officers	assigned	open	unmitigated	Retention risk: Medium probability if no adverse event after merger. Operational risk: Spend more on maintaining op co's competences Value risk: Not being focused on few high-value projects, lever 10 times ops risk
RESOURCE RISk—not enough IT staff to handle all projects the functional groups have planned around	**All**	T F Q	M	H	I, O: IT/systems	IT planning	assigned	open	unmitigated	Good project prioritization and planning needed
CHANGE MGT.—people may not align on priorities (productivity, what things to work on)	**All**	T F Q	M	M	I, O: IT/systems	CIO and project management.	unassigned	open	unmitigated	Good communication and buy-in is essential.
IT CULTURE—if people do not integrate then wars could arise	**All**	T F Q	L	M	I, O: IT/systems	New management.	unassigned	open	mitigated	Good communication and buy-in is essential.

Figure 1.3 HR risk list in the PCNet project

1.3 Risk Assessment and Prioritization

1.3.1. Impact Assessment: The Project Outcome Is a Distribution, Not a Number

After risks have been identified, their impact should be estimated, in order to prioritize them. For the large IT merger projects (from around $10 million), Max Schmeling built on the identified risk factors, and their possible values, to develop a probabilistic distribution of the project outcome. This was done with a scenario business plan with respect to the ultimate success measure, the NPV of savings (see Figure 1.4 for the PCNet project): "With only 10 percent probability, we will fail to deliver savings of at least $90 million; with 50 percent probability, we will not reach $135 million; and with 90 percent probability, we will not be able to deliver as much as $180 million in this project" (in other words, a pessimistic, medium, and optimistic scenario). The scenarios, connected to a value-distribution curve, were called P10, P50, and P90 (a method and terminology that come from mining and oil engineering). In the curve (Figure 1.4), the failure probability increases from left to right as the target increases. The value distribution for the PCNet project rested on similar curves for the four major subprojects.

The project value distribution curve in Figure 1.4 offers two benefits. First, it forces the team and management to acknowledge that the outcome cannot be planned exactly, as a number, but that many outcomes are possible with varying degrees of probability. In other words, the team cannot offer a fixed target, but only a confidence level (the probability of achieving $115 million in savings is 90 percent). Confidence levels offer a better understanding of the overall project riskiness than simplified project buffers that are used in other companies.

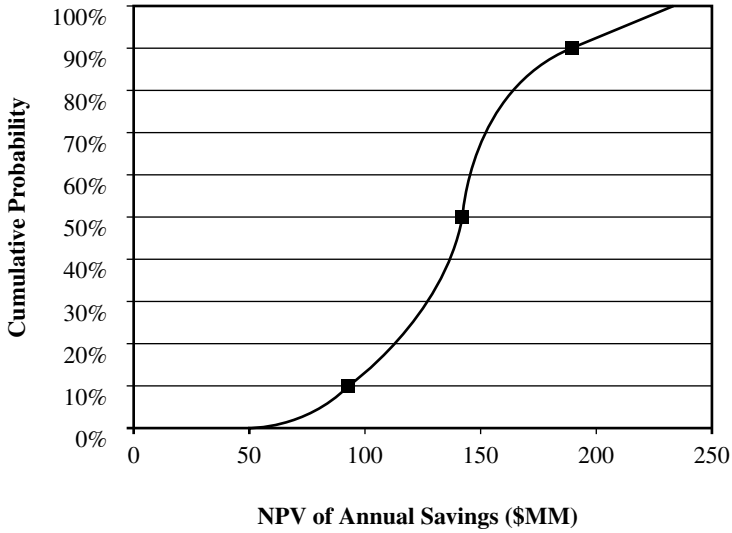


Figure 1.4 The PCNet project outcome distribution

Second, the value distribution curve offers a different dimension of priority for the key value drivers: The value distribution is influenced by the *variance* of the risk factors, and the distribution represents a "model" of how that variance impacts the project's value. This method is finer-grained than the expected impact that we have discussed above: Uncertain events often do not simply "occur or not occur" but have a continuum of possible values. For example, for the desktop migration subproject, the dominant risk lay in the prices set by the PC vendors. These prices had possible ranges, and the variance of the ranges defined the importance of the risk, both on the upside and the downside.

1.3.2 Risk Prioritization

Based on the impact assessment, risks are usually prioritized in order to allow the project team to focus attention on the most important ones. Typically, this prioritization is based on an "expected impact" of the risk, that is, size of impact, if possible in monetary terms, times probability of occurrence. However, one should not rely on this expected impact metric alone—a risk may have a moderate expected impact because it has a low probability; but at the same time, it may represent serious damage (a "showstopper") if it occurs. It may be advisable to pay keen attention to preventive or mitigating actions against such a risk.

In the PCNet project, hundreds of distinct risks were identified and listed in the risk planning process. They had to be prioritized in order to maintain focus (which was one of the main identified risks itself!) and efficiency. Rather than classifying the hundreds of risks themselves, the

merger team chose to classify the subprojects in a type of ABC analysis according to their value (that is, the amount at stake when a risk occurred) and the probability of failure (aggregated from individual risks affecting that project). The logic of this analysis is shown in Figure 1.5. The project management team aggressively intervened in high-priority projects (high value and high risk), whereas projects with high risk but low value were delegated to the Operating Companies, with an offer to help if requested. The well-running projects were either watched (high value) or let run (monitored only on a routine basis).

1.4 Risk Monitoring and Management

Risk identification and assessment form the basis on which the project can proactively influence the risks and monitor them, responding quickly if they occur. The Metal Resources Co. IT merger illustrates this.

1.4.1 Proactive Influencing of Risk Factors

The identification of the most important risk drivers by the value distribution curves (Figure 1.4) allowed the project team to manage them proactively. For the PC prices, the dominant risk for the desktop migration, a team of project managers visited the vendors and aggressively negotiated in order to lock in prices at a low level. Not only did this reduce the savings variance (guaranteed prices for all countries were obtained), but the centralized negotiation also achieved prices that were even lower than hoped for, creating additional savings. Thus, the pricing risk turned from a downside potential into a substantial upside opportunity, which was successfully utilized.

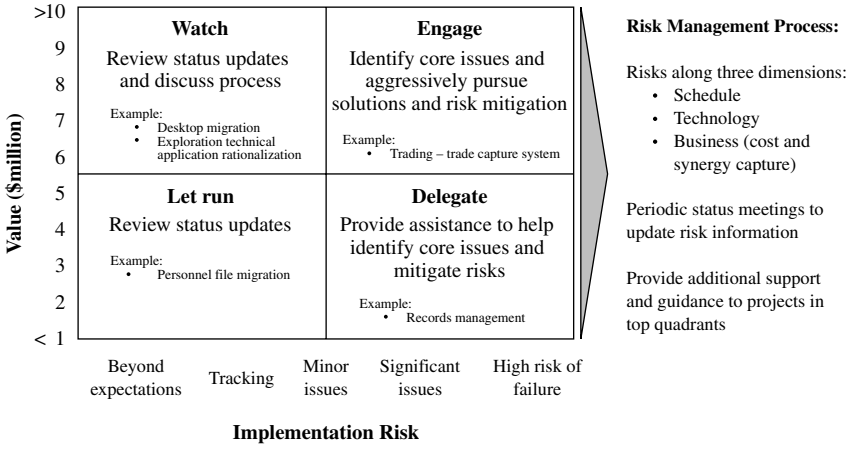


Figure 1.5 The Metal Resources Co. IT merger project prioritization

A second example relates to the considerable schedule risk of actually delivering all the desktops into all countries on time for the "new" system to start. Metal Resources Co. operated in countries such as Angola, Congo, or Armenia, where fighting might disrupt delivery, and where "gatekeepers," "consultants," or bureaucrats could block every move until permission is requested. Or sometimes they merely wanted to be shown attention and respect. In the aggregate, the schedule risk became large in such countries, or deployment might even be endangered entirely. So, for each country with significant bureaucratic restrictions, a plan was devised with countermeasures, emergency procedures, and appropriate buffers to allow for disruptions, and a deployment was not started until the remaining uncertainty had been reduced to a high confidence level such that the deployment could be carried out within the buffers allowed.

1.4.2 Monitoring and Reporting

Risk supervision concentrated on areas of high exposure. For example, the PCNet project came out as high priority from the classification in Figure 1.5: The desktop and server subprojects were in the upper right quadrant (high value and high risk), and the network project, while not directly of high value, was of high strategic importance and classified as high risk. The project team could not complain about a lack of attention from upper management.

In October 2002, work started in earnest, hitting multiple fronts at the same time: Telecom lines were rented and connected, network equipment was installed, security policies and software and directories were set up, and PCs were exchanged. Control of the large projects was paramount to keeping the integration on track and to producing the savings. An integration management office was set up for the merger as a whole (the "Integration Management Committee," of which Max Schmeling was a member), and the IT merger had its own integration office, the Project Management Office.

In monthly meetings, progress was tracked using the "Deployment Progress" monitoring tool (Figure 1.6). This reported on the progress status of PC deployment (for example, in January 2003, 1,428 of the 40,000 PCs had been migrated), sites with upgraded networks, reduced Internet access points to the global network, and reduced standard applications. The tool also showed the current budget status and offered comments on current events in the various regions of deployment.

In addition to the progress tool, which focused on operational figures, budgets and, of course, the financial synergies (or savings) were reported. The savings data were urgent: Only when they had been achieved and documented could they be incorporated into the accounting and bookkeeping systems, and then reported to external financial analysts. Being able to report booked synergies is very important for a CEO after an acquisition.

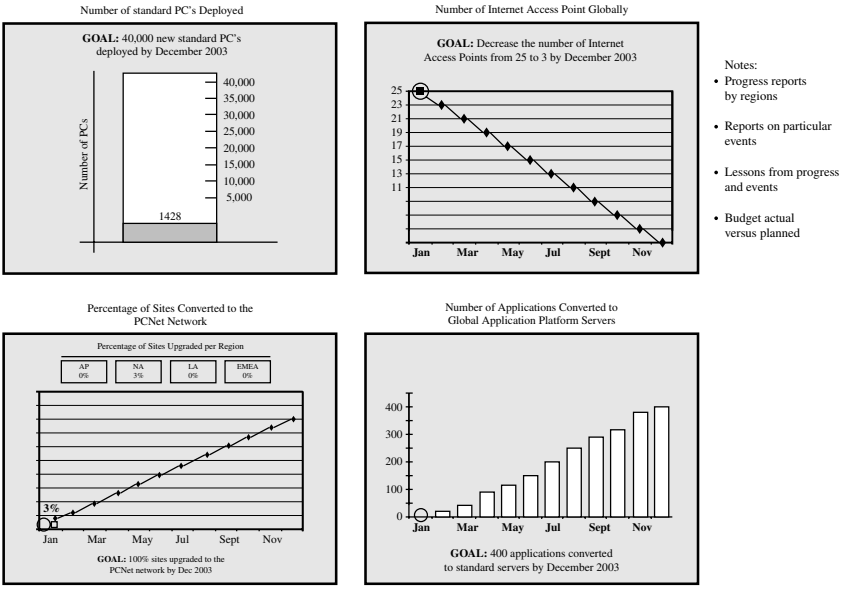


Figure 1.6 *Aggregate deployment progress monitoring tool*

During project execution, it became clear that the synergy progress reporting caused misunderstandings and tension. Real progress was made, not smoothly, but intermittently—for example, a site had to be completely migrated (up to three months' work) before savings really accrued, but then a large sum was saved at once. The synergy forecasts and targets, however, were "smoothed" and looked as if synergies were accruing at a regular rate every week. This caused an apparent deviation from the plan (a reporting artifact), as, for up to three months, it looked as if synergy capture was behind, before catching up. This required a lot of explanation: "Yes, although nothing has been booked, you have to trust us that the site migration is really on track and the savings will accrue as planned!" Reporting and education of the supervising committees had to go hand in hand.

1.5 Managing Residual Risks

The PCNet project had got off to a good start. However, in spite of all the thorough planning, "residual risk" began to plague the project. Residual risk took the form of nagging problems that kept arising out of the blue, none of them catastrophic in itself, but damaging nonetheless. In general, residual risk is not necessarily a sign of management problems: In a complex project, no planning, however thorough, can ever foresee all events; something not planned for will always happen. Therefore, it is key to building the capability of dealing with residual risk as it comes along. The PMI Standards Committee (1996) refers to this as "workarounds," and, if necessary, the PRM process is repeated if unexpected events occur.

In the PCNet project, the IT organization had managed on day one of the merger to build connectors between the two corporate networks, but there were no standards in place across the entire merged corporation. Thus, without rigorous change management processes in place, well-meaning people could (and did) introduce "tweaks" in, say, the e-mail system, unwittingly destabilizing an entire sector of the network. As a result, e-mail files were lost and messaging capabilities were corrupted. There were frequent small outages in some areas, which stubbornly persisted.

Moreover, some of Metal Resources Co.'s partner national companies suddenly demanded "local content," or "brokers," to be included in the channels of the hardware systems. These channel conflicts often caused delays and had to be mapped out and worked around, costing time and resources. A different problem occurred in Sri Lanka. The government partner, who was paying for the migration of 2,000 seats, decided that it would have to study the proposal thoroughly before giving its approval. This meant extra justification and a localized business case, again costing time and resources.

Unexpected problems came not only from the outside: Several business unit leaders within Metal Resources Co. slowed migration or postponed it from the original schedule, to avoid business disruptions or costs. One large European office threatened to delay a major deployment that had scheduling impacts on several other subprojects.

The Risk Management Office

To deal with residual risk, Max Schmeling built a formal structure, the Risk Management Office (RMO), complementing the Project Management Office (PMO). The PMO followed up on actions and reporting. The RMO focused on responding to deviations. It was a central control point, to which all teams were required to call in at least once a day to report on progress and problems that had arisen.

The RMO achieved two things. First, it represented a problem-solving resource—Metal Resources Co. had its own technical experts present in this center, plus experts on call from all technical areas at the main systems vendors (such as HP and IBM for PCs, Cisco for routers, Microsoft for operating systems, SAP for R3, EDS for the network operation, etc.), plus experts in culture and change management, who were also on call. Thus, when an unforeseen problem occurred, the center diagnosed it with the team in question and then helped to mobilize the expertise to bring about, or to plan, a solution as quickly as possible. Second, the quick information exchange offered a *fast spread of alarm bells (warnings) as well as of solution approaches*, across the many parallel teams. As many teams worked on very similar issues at multiple sites, a problem occurring at one site may well occur soon afterward at one or many of the other sites, and thus, warnings were relevant and a transfer of solutions was efficient. The quick communication of warnings from one team to another was dubbed "hot wire."

Thus, during each local deployment, a representative of the next local deployment team (in another state or another country) was present, so they became familiar with the logistical, as well as technical, issues. The Latin American deployment, for example, went very smoothly, thanks to this approach. Similarly, several problems that arose in the application migration to the new platform in Singapore were, once solved there, avoided throughout the Southeast Asian region.

Both the PMO and the RMO also attempted to prevent certain risks by enforcing strict standards (and thus reducing the complexity and number of things that could go wrong): For example, all of North America had to switch to a single SAP system configuration (there was a separate central control center for that project alone, which worked with all the organizational units to produce a common standard that satisfied most of the needs). Also, many technical and business software applications were standardized (such as statistical analysis packages, geological expert systems, etc.). Reducing the variety cut the number of different problems that could possibly arise and facilitated the spread of solutions across teams.

The RMO turned out to be very effective in responding to residual uncertainty. The problem of lost e-mails and corrupted e-mail capabilities, for instance, had to be attacked at two levels. The first level was technical—for example, when the lost files incidents were examined, the root problem turned out to be that Microsoft XP did not have a translator to automatically modify files. In response, the Microsoft developers made their own translator software available, which they used in-house. Installing this software systematically eliminated the problems and improved the overall network robustness. Several similar initiatives contributed to an overall network stabilization. The second solution level concerned change management processes: Over time, the merger team put such processes in place ("who can change what system features after discussing it with whom"), and over time convinced employees to comply with them, an initiative that eliminated incompatibilities introduced by local changes.

The Sri Lankan government partner eventually came on board, albeit at its own pace. This contributed to a six-month delay, but it did not "stop the show." The refining plant manager, who had refused the deployment, was won over with a combination of carrot and stick. The IT organization conducted a security audit at his site, which brought to light serious vulnerability to external attacks and other breakdowns. This allowed the team first to show him how awkward this might get for him locally (carrot) and, second, to make it clear to him that he would not be permitted to pose a risk for the rest of the organization (stick).

It turned out that the successful management of residual risks was crucial for the success of the project. The RMO was not simply a trivial variation on the general "risk monitoring and management" part of PRM. Installing the problem-solving capacity to respond to residual risks is fundamentally different from triggering ready-made responses to identified

risks. Therefore, we think that the standard PRM methodology that is summarized in Figure I.1 must be enhanced by the explicit managing of residual risk. We present this enhancement in Figure 1.7: Residual risk management is a distinct activity that is applied in parallel to the risk management phase. In contrast to risk management, it responds to unexpected events that require unplanned real-time problem solving.

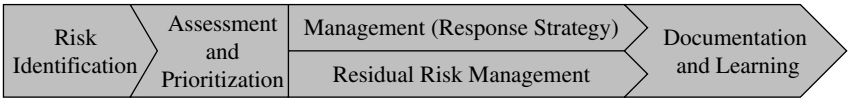
Our concept of residual risk management is consistent with Schoemaker's "strategic compass for profiting from uncertainty."[2] Schoemaker proposes a three-step process that prepares an organization for uncertainty. Although this approach is developed in a context of strategic planning, its philosophy has commonalities with our idea of handling residual risk: First, develop multiple future scenarios (to gain insight about the possibilities and uncover opportunities), develop a flexible strategy (that uses real options, analogous to the decision trees' ability to picture flexibility), and then monitor in real time and adjust to the unfolding future in a timely fashion (modifying the plan as you go along).

1.6 Learning and Sharing Across Projects

1.6.1 Learning over Time

The activities of the RMO enabled the organization to work with budget and schedule variances (deviations) in a more sophisticated way. For example, they performed variance analysis. There was significant overspending in Phase 3, because some work originally planned for Phase 4 had already been carried out at this point, and also because of many small "design changes," or improvements in protocols and processes that the organization implemented during the project. The activities of the RMO provided explanations for and documentation on residual risk and the respective responses.

Thus, the organization had a trace that allowed a thorough explanation of deviations, and an institutionalized effort to learn from the changes. One example of learning is the following: The early PC deployments took several man-days as the migration team was learning and stabilizing the components of the network. The later deployments required only a few hours (a reduction of 75 percent) and were much more stable.



- Emergency procedures
- Provision of expertise
- Real-time problem solving
- Adjustment of procedures
- Communication

Figure 1.7 PRM process enhanced by residual risk management

1.6.2 Learning from the Residual Risks

The solutions that the RMO developed were systematically generalized and transferred to other problems, which meant that the organization developed a codified and explicit set of solution methods. In other words, the organization learned from experience. As an example, the change management processes introduced in the context of the e-mail system stability enabled the IT organization to better manage the system.

Similarly, the cajoling and convincing of the refining plant manager was then crystallized into a standardized, compelling argument used in all interactions with operating managers who thought they had no time for offline activities like IT migration (Figure 1.8). The argument again combined the carrot and the stick: On the one hand, it explained the benefits to the operating units themselves and emphasized the fact that they could get help. On the other hand, the document threatened stakeholders with the withdrawal of support for their network if they did not migrate. This standard argument was, of course, accompanied by personal visits and face-to-face explanations.

1.6.3 Overall Success of the PCNet Project and Learning Applied to Other Projects

The IT organization learned how to execute the merger without disrupting ongoing operations, how to apply state-of-the-art methods, and how to deal with residual risks. In the end, no unexpected event was serious enough to break the project. The thorough planning, combined with the flexibility of the RMO and the hot wire, was so powerful that the huge IT merger undertaking became a convincing success.

The total IT merger project beat its target by $20 million, producing $230 million of synergies in the first year, and the PCNet project made a significant contribution to this overfulfillment (partially driven by an extra $10 million in PC discounts, the risk upside that came out of the proactive negotiations). Overall, the project remained slightly under budget, although it took six months longer than originally planned.

Documentation, in the form of a template, was produced, listing the major risks (downside and upside) that occurred. This template was applicable to other IT merger projects and continued to be used in the company.

1.7 PRM as a Method and as a Mind-Set

This chapter illustrates, we believe, that PRM is a powerful set of methods that help project organizations to anticipate and respond to risks. However, PRM is not something that an organization can simply decide to adopt overnight. As an illustration of this, we have worked with a number of organizations that could not take full advantage of PRM because management did not have the necessary mind-set.

The PCNet Deployment Consultant team presents . . .

The Top Ten List of *"Reasons why you should quickly and carefully decommission your legacy IT environment."*

10. Dual environments will make it more difficult to maintain IP compliance, particularly once Microsoft ceases support of NT 4.0.
9. Dual environments are impacting our networks due to unnecessary traffic from the legacy infrastructures such as file replication, Exchange Global Catalog replication, SMS inventory and package traffic, as well as WINS and DNS traffic.
8. Increased vulnerability to security attacks and viruses as vendors start dropping maintenance support for WIN9x, NT4 and W2K, and our internal, centralized efforts are no longer funded for these environments.
7. Increased cost for support as troubleshooting by support staff becomes a lot more complex due to having to follow separate processes and using different tools in order to support two environments. Cost also increases due to reduced reliability and increased break/fix calls as hardware has lived long past its planned life cycle.
6. Legacy Master Account X1 and X2 domains will be decommissioned, leaving unreliable domains. The old PC and workstation environments will lose connectivity. There will also be performance issues as Master Account domain controllers are removed.
5. The decommissioning effort is part of Metal Resources Co. and RBD synergy cost-savings and the realization of these savings now becomes our responsibility.
4. The business case for the synergies will be compromised by having to support dual infrastructures.
3. Manpower can be redirected toward strategic projects once the deployment and decommissioning efforts are completed (and we can take our vacations now!).
2. Old computing standards monthly cost will be increased by x2, x4, x6 the longer you keep your old hardware. Costs to maintain old infrastructure will be divided by the number of remaining old standard users.

And the #1 Reason is...

1. The old desktop **has** become "non-standard." Yes, it is true. The sun has set on the old standard, with the IT design team only providing Norton Anti-Virus updates and major security patches. ***Having old standard machines at your site makes your site "Non-Standard."***

   Here are three documents to help you in your efforts to decommission:
   Decommission Legacy Systems Guide
   Decommissioning Server Assets
   Decommissioning Workstation Assets

If the thought of pulling the plug on your favorite Compaq Proliant server is giving you nightmares and sleepless nights, then please e-mail me back about getting the PCNet Deployment Consultant team to offer decommissioning consulting services at your site.

Figure 1.8 Communication document for operating company compliance

Figure 1.9 (top) illustrates the mind-set with a metaphor: The traditional critical path mentality assumes that there is a well-defined target, and a path to get there, and the project must reach it; if obstacles are encountered or hostile winds distract the team, they'd better work harder at reaching the target or they will not have performed well. Take, as an example, the statement by one high-level manager who announced to his organization: "We need people who are reliable and fulfill targets. There are too many excuses

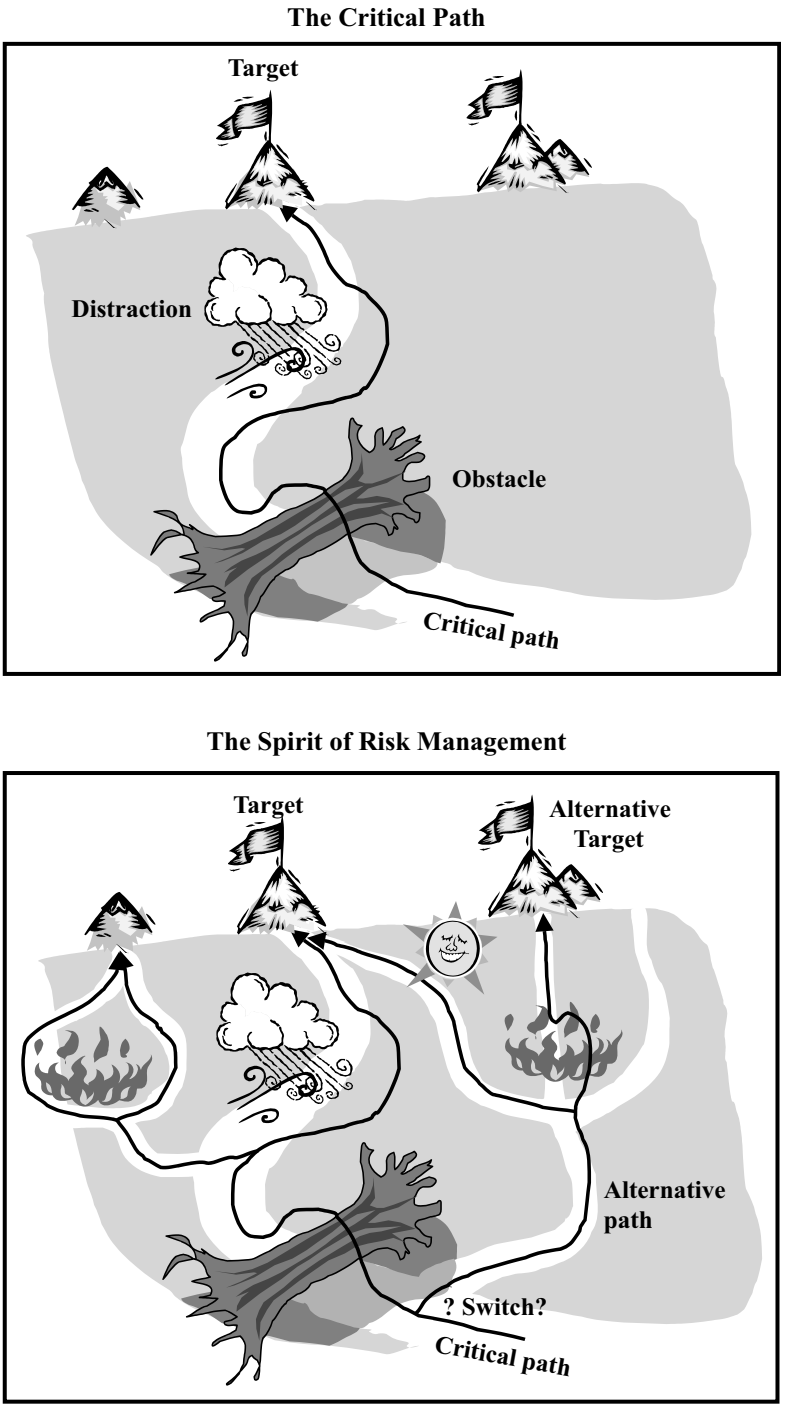


Figure 1.9 The critical path versus PRM mind-sets

and complications around here; we need people who simply get things done." In such organizations, allowing contingent actions and flexible targets makes management feel as if they are losing control. Project managers are "shot down in flames" when they propose contingent actions.

The bottom of Figure 1.9 illustrates the changed mind-set. Obstacles, alternative paths, and even alternative targets are identified and outlined at the outset, and a switch to the preventive/mitigating or contingent path (action) is triggered when the monitoring indicates that an obstacle has indeed occurred. Thus, PRM requires higher management sophistication—with PRM, targets and "getting things done" are fuzzier than a traditional organization is used to. Plans are more complex, monitoring is more difficult and subtle, and management must be sufficiently knowledgeable to understand when and why contingent action has been triggered.

Even more difficult is instilling awareness of residual risk (for example, the hostile wind that blows the project off course in Figure 1.9). A management that has not acquired the PRM mind-set, and does not understand the presence of residual risks, may revert to the critical path mind-set, punishing the team for running into trouble. We have seen organizations where the project teams did not trust supervising management to stay the course and built gigantic buffers into their plans, as a "private insurance" against residual risks. Sometimes, a game of "I cut your buffers" (management) versus "I build even bigger buffers" (project team) ensues, resulting in a total loss of planning and control.

The PCNet example in this chapter illustrates the power of PRM when it is competently executed, and when management uses it constructively. In the pharmaceutical, engineering services, chemical facilities, and power generation industries, and a few others, PRM has developed into a powerful way of guiding risky projects to success.

1.8 Summary and Conclusion

This chapter sets the baseline for this book by surveying the state-of-the-art in PRM. We have seen that PRM is a powerful method of achieving the stated project goals despite the risks. The method consists of four conceptual steps: (1) risk identification; (2) risk assessment and prioritization; (3) risk management with a collection of preventive, mitigating, and contingent actions; and (4) knowledge accumulation and transfer.

In the example of the Metal Resources Co. PCNet project, we saw the power of PRM in practice. In particular, the following lessons stand out:

- Thorough planning and anticipation is the foundation on which successful project management rests.

- Max Schmeling established responsibility for clearly defined outcomes, broken down to the task level. This accountability is the basis for project leadership.
- Risk planning is an integral part of project planning. Preparedness for deviations is the key to the team's ability to stay the course.
- Risk prioritization allows the team to stay focused. Focus is critical—once it is lost, the team will get bogged down and the project will stall.
- Transparency and clear communication of risks and progress status allows the team to remain coordinated and maintain a common direction. In a complex project, it is difficult to communicate risks, prioritization, and status in an easily understandable manner, but it is worth investing time and effort to accomplish this.
- Triggering planned responses to anticipated risks is not enough in challenging and complex projects. Residual risks will inevitably arise, as it is impossible to anticipate everything. Managing residual risk requires investing resources in real-time problem-solving capabilities (the RMO in the PCNet project). The standard PRM process must be enhanced by residual risk management (Figure 1.7).
- Successful PRM and residual risk management is not simply a method that can be routinely applied. It requires a management mind-set, in particular, the willingness to deal with unforeseen events constructively, without giving up the overall direction, and without blaming people.
- Learning and systematizing project experiences can improve execution, even within the same project, and can certainly benefit future projects in the same area.

We conclude with the question of whether the powerful method of PRM is the tool that can handle all projects, no matter how novel and complex. The answer, unfortunately, is no. The fundamental philosophy of PRM is still the achievement of stated goals, with a roughly agreed-upon approach, although it may change in detail. However, projects with high novelty (for example, a new market or a new technology) or high complexity (for example, many players with different sets of expertise, technologies, and expectations) may not have a (even roughly) defined target or approach. The rest of the book focuses on this added challenge. Chapter 2 illustrates an example where PRM is not enough. Chapter 3 begins to extend the PRM toolbox and mind-set.

Endnotes

1. This chapter is based on Loch 2005.
2. Schoemaker has summarized his approach in his book *Profiting from Uncertainty*.