White Paper

Risk Management

Too many managers believe that maintaining the risk register is synonymous with risk management, whilst having an effective risk register is important, it is only one part of an effective risk management system. Unfortunately, the core elements of risk management are set out in different ways in different standards and guides (some of the key ones are referenced below); they all include the basic steps set out in this White Paper but the language varies.

The basic Risk Management Processes

Initiating the Risk Management Process. Risks only exist in relation to defined objectives; therefore to frame any particular risk process you need to:

- Clearly defining the scope[1] and objectives[2] that are at risk (ie, the project or program scope and objectives).
- Define or ascertain the levels of risk key stakeholders are prepared to accept (their risk profile); this determines the target threshold for risk exposure.
- Identify any organisational assets or procedures that support or overlap with the current initiation.

Identify the Risks. Based on the defined scope and objectives, start identifying risks:

- Risks are uncertainties that might affect either the scope or the objectives, and includes both threats and opportunities.
- Organisations with effective knowledge management systems can use the 'lessons learned' on previous projects as the starting point.
- Use a variety of techniques to help find as many risks as possible.
- Record the risks in an effective risk register and identify a 'risk owner'.

Assess & Prioritise Risks. Risks should be analysed and prioritised for action. The assessment[3] process may be qualitative or quantitative. The outcome is a prioritised list of risks for action:

- Qualitative characteristics include:
  - How likely the event is to happen.
  - The likely effect on objectives.
  - How much influence we have on the event.
  - When the event may happen (near term or distant future).
- Quantitative methods use data to analyse risk exposure.
  - The magnitude of individual risks are calculated (time, value, other).
  - Contingency allowances for time and cost may be estimate based on the whole set of risks.

Determine Risk Responses (Planning). High priority risks that matter need to be actively managed. Planning determines who, what, when and how.

- Each risk needs an owner responsible for managing the risk.
- Appropriate responses should be determined and implemented by the risk manager.
- Response options include:
  - Establishing contingencies
  - Changing aspects of the project to enhance the likelihood of a benefit or mitigate the effect of a threat
  - Using contract provisions or insurances to transfer the effect to a third party.

---

[1] The scope should be outlined in the Charter, see: http://www.mosaicprojects.com.au/WhitePapers/WP1019_Charter.pdf

[2] For more on objectives see: http://www.mosaicprojects.com.au/WhitePapers/WP1042_Outputs_Outcomes_Benefits.pdf

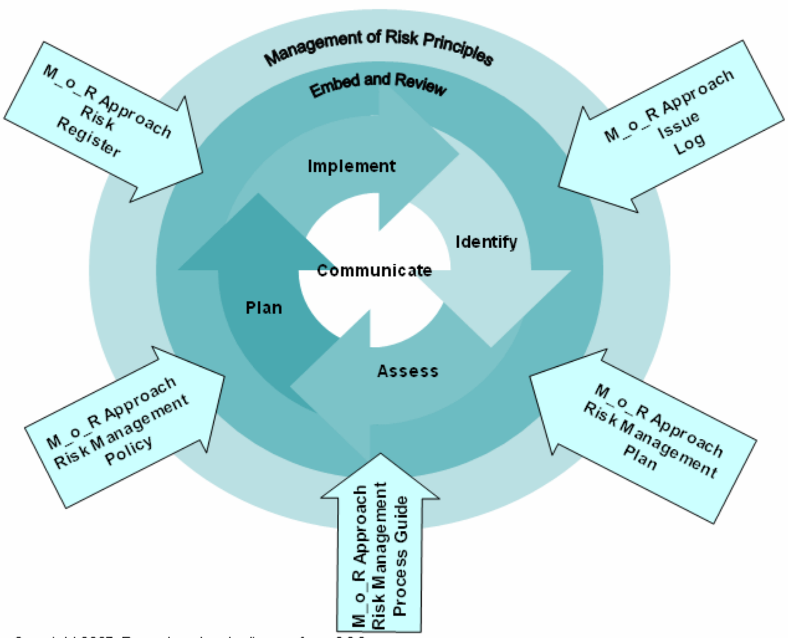
[3] For more on risk assessment see: http://www.mosaicprojects.com.au/WhitePapers/WP1015_Risk_Assessment.pdf

Risk Response Actions (Treatment). The planned responses must be implemented by the risk owner to change the overall risk exposure of the project.

- The implementation of each risk response should be incorporated in the project plan and actioned based on the plan.
- The results of each response should be monitored to ensure that they are having the desired effect.
- The consequence of the response may introduce new risks to be identified and addressed.
- Accepted risks, residual risks and unforseen risks may occur. The effect of a risk when it occurs has to be managed to maximise the benefits or minimise the consequences:
    - Risk response plans may be available for accepted risks, these should be implemented. (accepted risks are risks that have been identified but the cost of mitigating or avoiding the risk was deemed too high)
    - All other occurrences need to be proactively managed using 'workarounds'.
- Various stakeholders are interested in risk at different levels, and it is important to report to them on the risks and the plans to address them.

Risk Reviews. The overall risk profile of the project should be managed and reviewed on a regular basis. Topics for the review include:

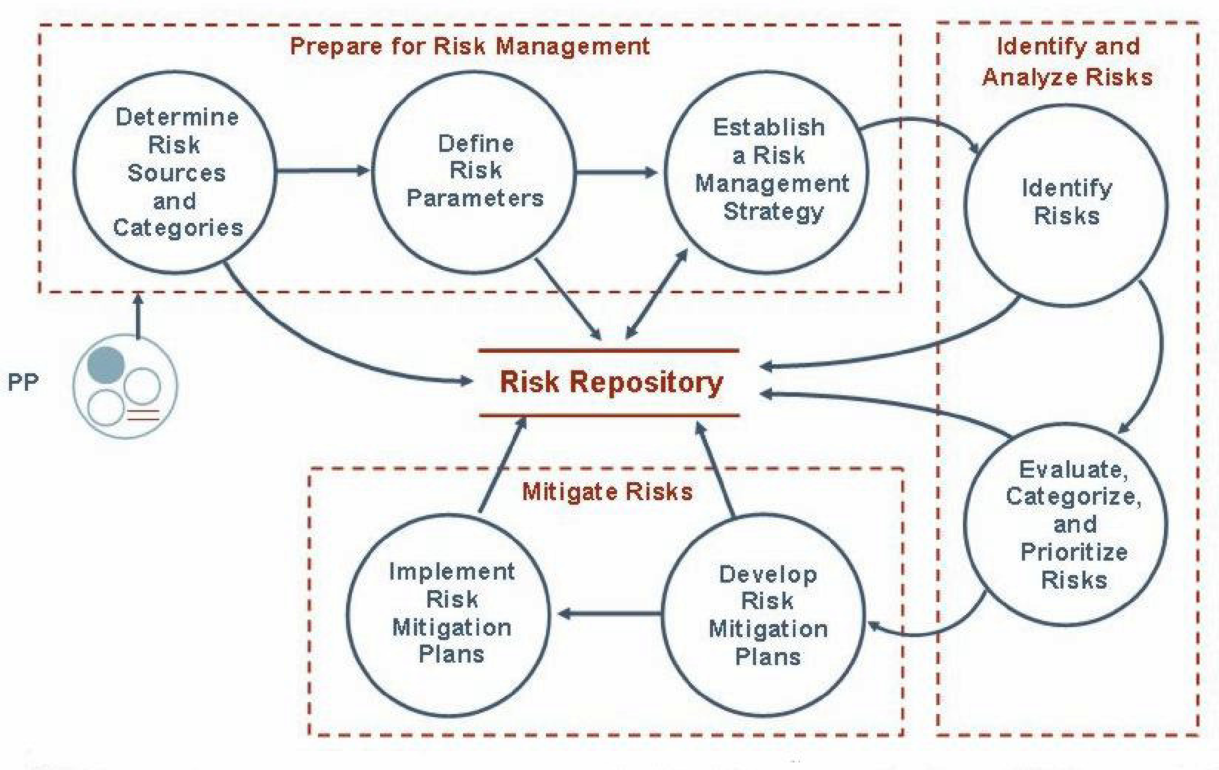
- Assessing whether the implemented actions have worked as expected.
- Monitor the consumption of reserves and contingencies as risk events occur
- Identify new and changed risks.
- Reprioritisation of all remaining risks.
- Assessment of appropriate treatments and actions.
- Appointment of a risk owner to any new risks (and any changes to existing risk owners).
- Inclusion of new or revised treatments into the overall project plan for action.



The M_o_R Framework for Risk Management

Overall Risk Management. Risk management is part of the overall governance structure of the organisation. The project and program risk processes should be part of and integrate with the organisations risk management system. Some of the key elements include:

- Capturing lessons learned. At the end of the project or program, or after a risk event has occurred; time should be taken to think about what worked well and what needs improvement, and record the conclusions in a way that makes the lessons learned readily available in an effective knowledge management system.
- Reporting and understanding systemic risk factors and the impact of the project's risks on the overall organisation's risk profile
- Supporting organisational Audit and compliance requirements through accurate and transparent risk recording and reporting processes.



The Risk Management (RSKM) Process Area of CMMI

Risk Management Standards

Published standards and guide assist in developing an effective risk management system for the organisation. Some of the key risk management standards include:

- ISO 31000 Risk Management. ISO 31000 is intended to be a family of standards relating to risk management. Available from SAI: http://infostore.saiglobal.com/store/
- AS/NZS 4360:2004, Risk management. The Australian standard for risk management including guidelines. Available from SAI: http://infostore.saiglobal.com/store/
- PMI Practice Standard for Risk Management. Supports and extends the risk management aspects of the *PMBOK® Guide* 4th Edition. Available from PMI USA, Amazon and the PMI Melbourne Chapter at: http://www.melbourne.pmi.org.au/catalog.aspx?cid=2
- Project Risk Analysis and Management (PRAM Guide). Available from The Association for Project Management (UK): http://www.apm.org.uk/
- Prioritising Project Risks, A short guide to useful techniques. Available from The Association for Project Management: http://www.apm.org.uk/
- Interfacing Risk and Earned Value Management. Available from The Association for Project Management: http://www.apm.org.uk/
- Management of Risk (M_o_R). Available from Office of Government Commerce (OGC): http://www.mor-officialsite.com/home/home.asp