

# Risk Management

The international risk standard ISO31000:2009 Risk Management - Principles and Guidelines says risk is **'effect of uncertainty on objectives'**, and the Project Management Institute *Practice Standard for Project Risk Management* defines risk as an **'uncertain event or condition that, if it occurs, has a positive or negative effect on a project's objectives.'** For each of your project's objectives there are also likely to be risks that might affect them!

Managing these risks is important because it focuses attention on the uncertainties that matter. Unfortunately, too many managers believe that offloading the risk management process to a 'Risk Manager' or maintaining the risk register is synonymous with risk management, whilst having an effective risk register is important<sup>1</sup>, it is only one part of an effective risk management system. Similarly, it is helpful for someone to be responsible for running the risk processes, to make sure that it happens smoothly and effectively, to ensure adherence to standards, to encourage and inspire people to be involved and committed to managing risk, and to coordinate data management and risk reporting. However, it is misleading to call this person *the Risk Manager*. A more accurate job title could be: Risk Coordinator, Risk Facilitator, Risk Champion or Risk Process Manager. These names explain what the role actually does and prevents people from expecting someone else to manage their risks for them. Given any specific risk is an **uncertainty that matters**, then the risk only matters to the person whose objective is at risk. And that person should take responsibility for managing the risks that affect their objectives (although they might involve other people to help them) by implementing the processes defined in this White Paper.

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<sup>2</sup> and objectives<sup>3</sup> 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 (see sub-heading below: *The Principles of Effective Risk Management*).

**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'<sup>4</sup> 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<sup>5</sup> process may be qualitative or quantitative. The outcome is a prioritised list of risks for action:

---

<sup>1</sup> For a simple risk register see: [http://www.mosaicprojects.com.au/Tools+Template\\_Sales.html#Risk](http://www.mosaicprojects.com.au/Tools+Template_Sales.html#Risk)

<sup>2</sup> The scope should be outlined in the Charter, see: [http://www.mosaicprojects.com.au/WhitePapers/WP1019\\_Charter.pdf](http://www.mosaicprojects.com.au/WhitePapers/WP1019_Charter.pdf)

<sup>3</sup> For more on objectives see: [http://www.mosaicprojects.com.au/WhitePapers/WP1042\\_Outputs\\_Outcomes\\_Benefits.pdf](http://www.mosaicprojects.com.au/WhitePapers/WP1042_Outputs_Outcomes_Benefits.pdf)

<sup>4</sup> For more on Lessons Learned see: [http://www.mosaicprojects.com.au/WhitePapers/WP1004\\_Lessons\\_Learned.pdf](http://www.mosaicprojects.com.au/WhitePapers/WP1004_Lessons_Learned.pdf)

<sup>5</sup> For more on risk assessment see: [http://www.mosaicprojects.com.au/WhitePapers/WP1015\\_Risk\\_Assessment.pdf](http://www.mosaicprojects.com.au/WhitePapers/WP1015_Risk_Assessment.pdf)

- 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).
  - Anticipate the incidence of recurring problems by using the concept of risk coefficients. Risks, such as bad weather, illnesses, tasks taking longer (or occasionally less) than planned, and changes, are so frequent that organisations often have statistics on their occurrence. Good plans model their occurrence and incorporate their effect.
  - 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.

**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 unforeseen 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.

**Regular 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 Principles of Effective Risk Management

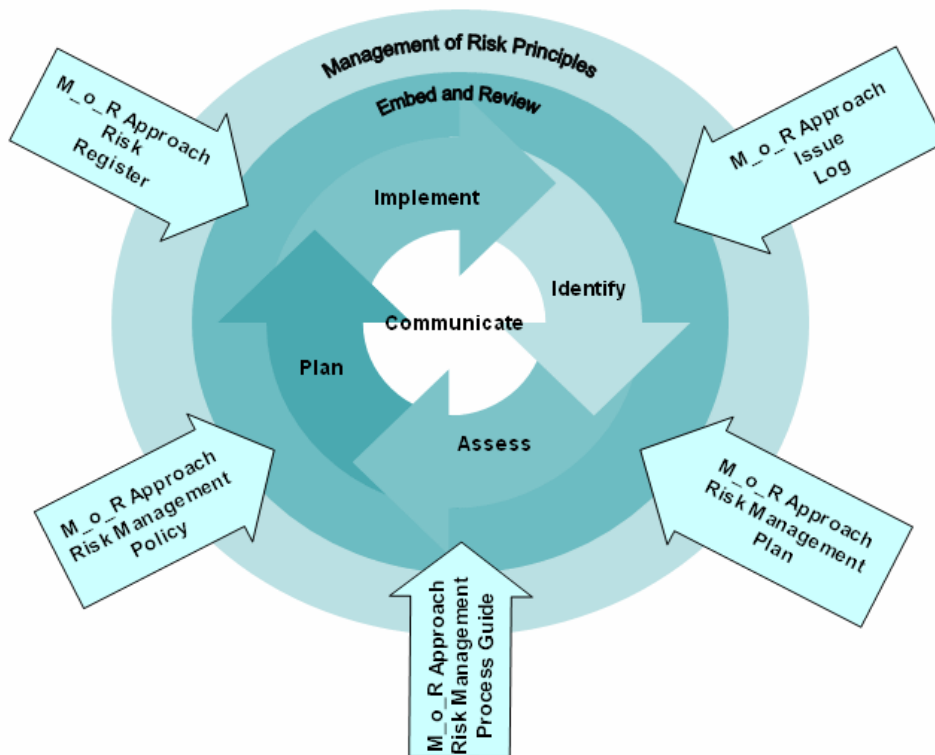
The OGC M\_o\_R risk principles<sup>6</sup> have very broad applicability:

1. **Risk management aligns continually with organisational objectives.** Risk is *uncertainty that matters*, and it only matters if it could affect achievement of the objectives of the organisation. We need to understand our objectives, define how much risk is acceptable, and decide how to manage risk within those limits. When objectives or risk tolerances change, the risk process must change too.
2. **Risk management is designed to fit the current context.** Organisations operate in an external context (markets, competition, regulation etc.) as well as an internal context (culture, people and processes). Risk management must recognise and respond to the context, and change when it changes.
3. **Risk management engages stakeholders and deals with differing perceptions of risk.** Different stakeholders see risk differently, and the risk approach must take account of these perceptions. We need to recognise and counter bias, and manage stakeholder expectations regarding risk.
4. **Risk management provides clear and coherent guidance to stakeholders.** Clarity means that everyone knows what the risks are and how they are being addressed. Coherence occurs when risk is managed consistently across all levels of the organisation, and when it is communicated properly across organisational boundaries.
5. **Risk management is linked to and informs decision-making across the organisation.** We have to make decisions with incomplete or imperfect information, which makes decisions risky. The best decisions are made when we understand the risks that are associated with different options.
6. **Risk management uses historical data and facilitates learning and continual improvement.** We can improve the way we manage risk by identifying generic sources of risk and developing effective generic responses. The aim is to become more mature in our risk culture and practice.
7. **Risk management creates a culture that recognises uncertainty and supports considered risk-taking.** Every significant activity involves uncertainty and requires us to take risk. But we need to take the right level of risk, balancing risk-taking with reward. This requires a risk-mature culture that rewards proactive risk management.
8. **Risk management enables achievement of measurable organisational value.** The risk process should result in fewer threats turning into real problems. It should also help us to turn more opportunities into real benefits. Both of these will create measurable value for the organisation.

The OGC M\_o\_R principles provide a framework to challenge the way organisations manage (not avoid) risk. ISO31000:2009 (below), covers similar territory, but as 11 principles.

---

<sup>6</sup> OGC M\_o\_R: UK Office of Government Commerce (OGC). 2010. Management of Risk: Guidance for Practitioners (third edition). London, UK: The Stationery Office. ISBN 978-0-11-331274-0



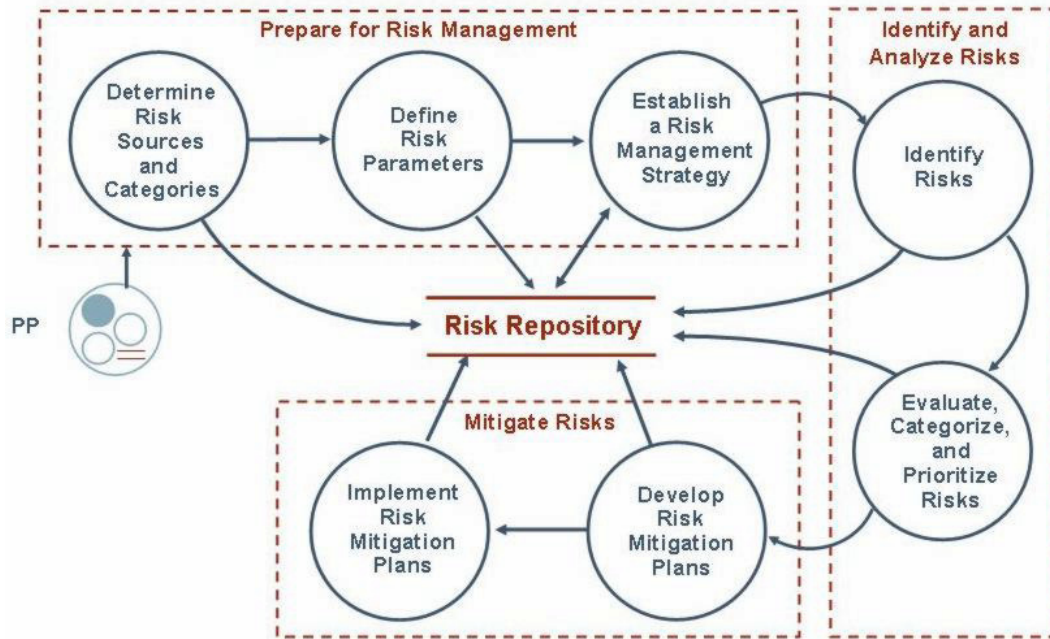
© Crown Copyright 2007. Reproduced under licence from OGC.

### The M\_o\_R Framework for Risk Management

- The core principles defined in **ISO 31000:2009 Risk Management - Principles and Guidelines** are:
  1. **Risk management creates and protects value.** Value is created when we achieve our objectives, and risk management helps us to optimise our performance. It also protects value by minimising the effect of downside risk, avoiding waste and rework.
  2. **Risk management is an integral part of all organisational processes.** Risk management is not a stand-alone activity, and it should be "built-in not bolt-on". Everything we do should take account of risk.
  3. **Risk management is part of decision-making.** When we are faced with important situations that involve significant uncertainty, our decisions need to be risk-informed.
  4. **Risk management explicitly addresses uncertainty.** All sources and forms of uncertainty need to be considered, not just "risk events". This includes ambiguity, variability, complexity, change etc.
  5. **Risk management is systematic, structured and timely.** The risk process should be conducted in a disciplined way to maximise its effectiveness and efficiency.
  6. **Risk management is based on the best available information.** We will never have perfect information, but we should always be sure to use every source, being aware of its limitations.
  7. **Risk management is tailored.** There is no "one-size-fits-all" approach that suits everyone. We need to adjust the process to match the specific risk challenge that we face.
  8. **Risk management takes human and cultural factors into account.** Risk is managed by people not processes or techniques. We need to recognise the existence of different risk perceptions and risk attitudes.
  9. **Risk management is transparent and inclusive.** We must communicate honestly about risk to our stakeholders and decision-makers, even if the message is unwelcome to some.
  10. **Risk management is dynamic, iterative and responsive to change.** Risk changes constantly, and the risk process needs to stay up to date, reviewing existing risks and identifying new ones.
  11. **Risk management facilitates continual improvement of the organisation.** Our management of risk should improve with time as we learn lessons from the past in order to benefit the future.

**Organisational Governance.** Risk management is part of the overall governance structure of the organisation<sup>7</sup>. 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<sup>8</sup>. 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.



**The Risk Management (RSKM) Process Area of CMMI**

- 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.

**Unplanned Risk Events**

It is impossible to know what you do not know. Many risk events will occur during the course of the project that were not identified, listed or planned<sup>9</sup>. For any organisation, system, or project team to withstand the impact of unexpected events two elements are needed. First the team needs to have a level of resilience that allows the impact to be absorbed, managed and dealt with. Building resilience into any team or system is not simple and requires an organic capability to respond creatively and effectively. The team and system need some spare capacity (even if this is achieved by extraordinary effort), good internal communications, trust in each other and a clear understanding of how things work.

The second element is practiced agility in dealing with potential scenarios. The actual event will be different to the scenarios practiced but the response processes should be established. Some of the key elements include:

- Senior management commitment to support the team

<sup>7</sup> For more on governance see: [http://www.mosaicprojects.com.au/WhitePapers/WP1033\\_Governance.pdf](http://www.mosaicprojects.com.au/WhitePapers/WP1033_Governance.pdf)

<sup>8</sup> For more on lessons learned see: [http://www.mosaicprojects.com.au/WhitePapers/WP1004\\_Lessons\\_Learned.pdf](http://www.mosaicprojects.com.au/WhitePapers/WP1004_Lessons_Learned.pdf)

<sup>9</sup> For more on unknown unknowns see: [http://www.mosaicprojects.com.au/WhitePapers/WP1057\\_Types\\_of\\_Risk.pdf](http://www.mosaicprojects.com.au/WhitePapers/WP1057_Types_of_Risk.pdf)

- Established processes and a core administrative team
- A rapid response plan that may include:
  - o Classification and trigger points – you need to recognise you have a problem
    - A medical emergency
    - A system failure
    - An external threat – fire, bomb, storm, etc
  - o Call out procedures to assemble the response team
  - o Immediate actions to protect and preserve
  - o Team roles and responsibilities
  - o Strategies to deal with foreseeable threats
  - o Strategies to deal with stakeholders, the media and regulatory authorities
  - o Recovery and continuity plans

There is no point in having a plan if it is not practiced, rehearsal and drills are important. Depending on the severity of the risk options include desk-top exercises through to full dress rehearsals. Risk management and crisis management are closely aligned – a significant risk event will trigger a crisis.

## 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* 4<sup>th</sup> Edition. Available from PMI USA, Amazon and Mosaic (Australian sales): [http://www.mosaicprojects.com.au/Book\\_Sales.html#PMI](http://www.mosaicprojects.com.au/Book_Sales.html#PMI)
- 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>