Risk Management

Managing risks is important because it focuses attention on the uncertainties that matter. 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.'*** These definitions implicitly contain three elements:

- An ***uncertain event or condition*** (situation) that may occur in the future;
- The ***likelihood of occurrence*** of the situation; and
- The ***effect*** (positive or negative) that the occurrence would have on one or more of the project's (or program's) objectives.

For each objective there are likely to be various risks of different types[1] that might affect it:

- Known-Knowns are in the plan
- Known-Unknowns are in the risk register
- Unknown-Unknowns are unidentified risks
- Unknown-Knowns are the mistakes embedded in the plan!

Who Manages Risk?

The short answer is everyone, starting from the 'Governing Body' and the executive. 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; this is a dangerous misconception - whilst having an effective risk register is important[2], it is only one part of an effective risk management system. Certainly, it is important 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.

An equally dangerous proposition is establishing a 'Chief Risk Officer' with a centralised 'control' of the risk management processes. The function of the CRO's office should be to oversee the functioning of the 'enterprise risk management' (ERM) system and liaise with the governing body; not the centralised management of 'all risk' which easily can lead to non-realistic outputs. An effective ERM system decentralises the management of risk through the creation of a coherent top-down hierarchy of objectives at multiple levels throughout the business, with lower-level objectives aligned to the strategic objectives of the overall organisation. It is then possible to manage risk at each level, linking risks to the objectives at that level. The function coordinates the various levels of risk management, ensuring that common standards are applied, and escalating risks as required. The organisation's overall risk policies and standards should be set at ERM level, allowing lower levels of organisation the freedom to tailor their risk approach within the overall minimum requirements set by ERM and to develop their own specific risk procedures to deal with specific circumstances. Effective risk management is not 'one-size-fits-all' function.

The reason decentralisation is important is that given any specific risk is an ***uncertainty that matters***, then the risk only really 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 ERM system and discussed in this White Paper.

[1] For more on the ***types of risk*** see: http://www.mosaicprojects.com.au/WhitePapers/WP1057_Types_of_Risk.pdf

[2] For a ***simple risk register*** see: http://www.mosaicprojects.com.au/Tools+Template_Sales.html#Risk

First published: 13th August 2010 – extensively augmented and updated.

The right culture is needed to support the effective management of risk which is of itself a governance issue[3]. The culture has to 'allow' people to identify, quantify and manage the real risks even if they are politically unpopular. This needs a change of perspective, away from risk management and towards risk leadership[4]. Risk leadership is needed to develop and maintain an effective risk culture within an organisation by:

- Giving overall strategic direction and vision in relation to risk and setting the right ethical and governance framework.
- Defining the risk appetite for the organisation, providing the broad outline of how risk will be addressed, how much risk is acceptable, and what degree of risk exposure will be tolerated.
- Identifying and requiring appropriate risk management processes (see below).
- Leading by example and modelling a mature approach to risk and using the risk management processes as a tool rather then a straightjacket by demonstrating a flexible risk attitude, being prepared to take risk when that is appropriate and prepared to act more cautiously if necessary.
- And inspiring the same flexibility in others by rewarding good risk management behaviour and encouraging people to adopt the right risk attitude to meet each changing circumstance. The skill is identifying the 'right risks' to accept that allow growth and improvement and managing these effectively. Trying to avoid 'all risk' is impossible, and a recipe for failure.

Accepting risk means accepting the possibility of failure but this approach is far better then pretending there are no risks or that every risk can be managed to the point where it is inconsequential.

Risk Management Processes

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.

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[5] and objectives[6] 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 appetite); this determines the target threshold for risk exposure.
- Develop a risk management plan that defines the scope, objectives and parameters of the risk process to be used on the project and the responsible managers. (see sub-heading below: *Defining the appropriate level of Risk Management*).
- 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 of the work, and includes both threats and opportunities.
- Organisations with effective knowledge management systems can use the 'lessons learned[7]' on previous projects as the starting point.
- Use a variety of techniques to help find as many risks as possible.

[3] For more on ***governance*** see: http://www.mosaicprojects.com.au/WhitePapers/WP1084_Governance_Systems.pdf

[4] For more on ***leadership*** see: http://www.mosaicprojects.com.au/WhitePapers/WP1014_Leadership.pdf

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

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

[7] For more on ***Lessons Learned*** see: http://www.mosaicprojects.com.au/WhitePapers/WP1004_Lessons_Learned.pdf

- The use of 'risk metalanguage' in the form: **If a** *<one or more causes>***, caused by** *<uncertain situation>* **occurs, it may cause** *<one or more effects>*.
- Record the risks in an effective risk register[8] and identify a 'risk owner'.

Assess & Prioritise Risks. Risks should be analysed and prioritised for action. The assessment[9] 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.
    - How easy is the risk to detect as it is emerging? Easy to detect risks (obvious early warning indicators) are easier to deal with than risks that just 'happen' without warning.
    - 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.
    - Probability can be separate or cumulative[10].
    - Contingency allowances for time and cost may be estimate based on the whole set of risks[11].
- The risk statement can now be expanded to include: **If a** *<one or more causes>***, caused by** *<uncertain situation>* **occurs, it may cause** *<one or more effects>*. **The impact of this** *<threat / opportunity>* **is** *<assessed affect on objectives>***.**

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 owner[12].
- 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 (opportunity or threat) to a third party; or

---

[8] For an example of a ***simple risk register*** see: http://www.mosaicprojects.com.au/Tools+Template_Sales.html#Risk

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

[10] For more on ***probability*** see: http://www.mosaicprojects.com.au/WhitePapers/WP1037_Probability.pdf

[11] Contingencies may be created/held for identified (and quantified) risks – the 'known unknowns'. Provided there is no doubling up some risks exist at the work package level, some across a group of work packages (ie, control account level) and some at the project level. The contingency (cost or time) needs to be allocated at the appropriate level to offset the effect of the risk it was created to compensate for. Some contingency can be distributed early in the planning process for risks that clearly affect a work package or control account (ie, work area). Most of the contingency is held at the project level and distributed after the event to offset the consequences of a risk that has eventuated. Contingencies form part of the project baseline, a separate management reserve may be included in the overall project funding but held outside of the baseline to compensate for 'unknown unknowns'; these reserves are only released to the project through a formal change control process. As work progresses and/or more information becomes available the contingencies may be used, reduced or eliminated.

[12] **Note:** if the risk exceeds the tolerances allowed for the project and cannot be avoided, transferred or mitigated, and/or it affects other parts of the organisation, management of the risk should be escalated to the appropriate management level for direction or management.

First published: 13th August 2010 – extensively augmented and updated.

- Changing the project to eliminate threats by not doing whatever causes the threat, or to lock in opportunities so they do occur.
- Escalating risks we have identified that may not affect our objectives, but that could affect some other part of the organisation. Risk escalation is used to pass the risk to the person or party who would be affected if the risk (opportunity or threat) happened – organizational systems are needed with designated thresholds and contact points defined for effective risk escalation.

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 action taken 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 (secondary risks).
- Accepted risks, residual risks (any risk remaining after treatment) 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.

Risk Communication: Inform stakeholders about the current risk exposure and its implications for project success.

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.
- Recognising *sentinel events*[13]
- Reprioritisation of all remaining risks.
- Assessment of appropriate treatments, actions and escalations v.
- 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.

Lessons-Learned Review: As part of the overall project 'lessons learned' process, identify risk-related lessons to be learned for future projects

Issues Management: Realised risks become issues - an issue is a risk with a 100%probability of occurring, either because it has already happened or because it will inevitably happen in the near future. The issues management process may be integral to the risk management process or a separate process. In either situation, the preparatory planning undertaken during risk management is actioned to minimise the impact of the risk event[14].

[13] For more on ***sentinel events*** see:
http://www.mosaicprojects.com.au/Mag_Articles/P019_Risk_Reassessment-Sentinel_Events.pdf

[14] For more on ***Issues Management*** see:
http://www.mosaicprojects.com.au/WhitePapers/WP1089_Issues_Management.pdf

Defining the appropriate level of Risk Management

Projects and programs are exposed to different levels of risk, so the risk management process needs to be appropriately adapted to meet the risk challenge. Scaleable elements include:

- **Risk responsibilities.** In the simplest case the project manager may undertake all the elements of the risk process as part of their overall responsibility for managing the project, without using a risk specialist such as a Risk Champion or Risk Coordinator. At the other extreme a complex risky project may require input from people with particular risk skills, and a dedicated risk team may be employed, either from within the organisation or from outside.
- **Methodology and processes.** A low-risk project may be able to incorporate the risk process within the overall project management process, without the need for specific risk management activities. A more risky project may need to use a defined risk process, perhaps following a recognised risk methodology.
- **Tools and techniques.** The simplest risk process might involve a team brainstorm as part of another project meeting recording risks in a word document, and monitoring actions through the regular project review meetings. More risky projects may require a series of meetings, a spreadsheet[15] with some basic calculations and mitigation plans with assigned risk 'owners'. The most risky projects may require a wide range of techniques and specialist tools for risk identification, assessment and control, to ensure that all aspects of risk exposure are captured and dealt with appropriately.
- **Supporting infrastructure.** The lowest-risk projects may require no dedicated risk infrastructure, whereas high-risk projects demand robust support from integrated toolkits with high levels of functionality. It is important to get the level of infrastructure right as too much support can strangle the risk process and too little support can leave it unable to function.
- **Reporting requirement.** For some projects the risk reporting can be incorporated into routine project reports, whereas others may demand a variety of specific risk reports targeted to the needs of different stakeholders, providing each group of stakeholders with risk information that matches their interest in the project.
- **Review and update frequency.** It may be sufficient on low-risk or short duration projects to update the risk assessment only once or twice during the life of the project. Other projects which are more risky or of longer duration may need a regular risk update cycle, say monthly or quarterly, depending on the project's complexity and rate of change.

Decisions on each of these scalable aspects should be documented in the project's Risk Management Plan, as part of the Risk Process Initiation step and agreed with the sponsor or client.

Dealing with Opportunities

Typically, about 80% or more of the risks recorded in Risk Registers are threats (negative risks), with less than 20% opportunities (positive risks) – ideally this needs changing! Even if you cannot completely reverse the 80/20 balance, you need to work to fundamentally change the attitudes of internal stakeholders towards risk identification.

Actively seek opportunities. To promote this approach, ask your teams to view their project as a bank account. Every threat corresponds to a withdrawal or an additional charge, and each opportunity is a deposit or added income. Most people understand that, to preserve and enhance the overall value of their account, it is important to focus on increasing gains as well as reducing charges. To achieve this you need to encourage people to take risks.

Set opportunity-based risk thresholds. Asking people to take risks requires limits to be of what is acceptable. All business investments and projects are carried out to create value for stakeholders. Risk thresholds can only be determined by considering the potential for both value creation and value destruction for the organisation and using this to define acceptable risk thresholds. Based on these values, people can concentrate on maximising value creation through controlled risk-taking.

[15] For an example of a ***risk management spreadsheet*** see: http://www.mosaicprojects.com.au/Tools+Template_Sales.html#Risk

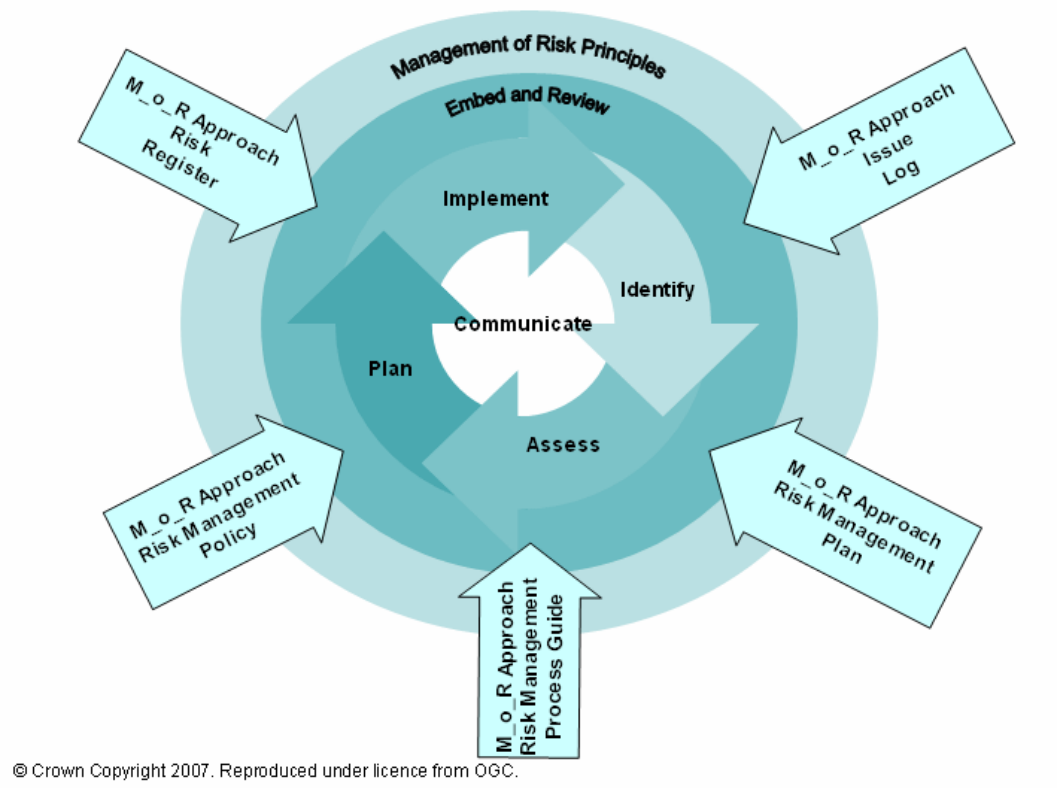
First published: 13th August 2010 – extensively augmented and updated.

Use value-focused risk management. Value is defined as: *any desirable result for a stakeholder in a given context*[16]. Once the anticipated value is defined risk process can be focused on enhancing the main value-creating opportunities, while at the same time addressing the principal threats that would undermine value for stakeholders.

Implement success-oriented risk response planning. Focus risk management on taking action in order to win, rather than hoping not to lose! In the traditional threat-based approach to risk management, people aim to protect themselves at all costs; this purely precautionary approach is always inefficient, and often ends up protecting from things that are unlikely to happen. By focusing action plans on creating value, it creates a win-win situation with the stakeholders involved.

The Principles of Effective Risk Management

The OGC M_o_R risk principles[17] have very broad applicability:



The M_o_R Framework for Risk Management

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.

[16] For more on ***value realisations*** see: http://www.mosaicprojects.com.au/WhitePapers/WP1023_Benefits_and_Value.pdf

[17] 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

First published: 13th August 2010 – extensively augmented and updated.

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.

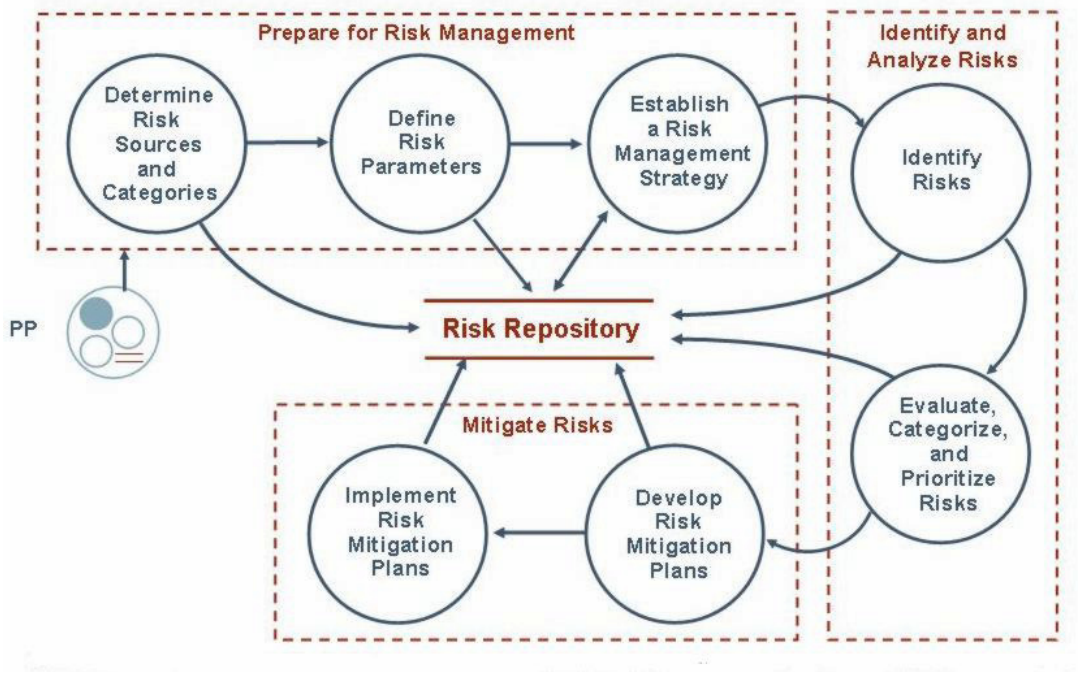
The OGC M_o_R principles provide a framework to challenge the way organisations manage (not avoid) risk. ISO31000:2009 (below), covers similar territory, but as 11 principles.

- 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.

First published: 13th August 2010 – extensively augmented and updated.

Organisational Governance. Risk management is part of the overall governance structure of the organisation[18]. The project and program risk processes should be part of and integrate with the organisations risk management system. Some of the key elements include:



The Risk Management (RSKM) Process Area of CMMI

- Capturing lessons learned[19]. 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.

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[20]. 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:

- Senor management commitment to support the team

[18] For more on ***governance*** see: http://www.mosaicprojects.com.au/WhitePapers/WP1033_Governance.pdf

[19] For more on ***lessons learned*** see: http://www.mosaicprojects.com.au/WhitePapers/WP1004_Lessons_Learned.pdf

[20] For more on ***unknown unknowns*** see: 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:
  - 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
  - Call out procedures to assemble the response team
  - Immediate actions to protect and preserve
  - Team roles and responsibilities
  - Strategies to deal with foreseeable threats
  - Strategies to deal with stakeholders, the media and regulatory authorities
  - 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 Health Checks

An effective risk culture that proactively identifies all risk and accepts the right risks to support the development of the organisation is a core business activity. The key questions the 'governing board' need to ask regularly are:

1. Does everyone speak the same 'risk language' and understand the risk culture of the organisation?
2. Has risk management degenerated into a 'box ticking' process or a 'form-filling' bureaucracy? Or is there proactive debate over key risk decisions?
3. Do we have the right controls in place or are there too many restrictions?
4. Do we learn from our mistakes and improve the system by sharpening focus or does another layer of bureaucracy get added each time a mistake is identified?
5. Does our risk management framework extend to our strategic decision making, and align with our strategic objectives?
6. Is everybody accountable for managing their risks?

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 Mosaic (Australian sales): 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/

First published: 13th August 2010 – extensively augmented and updated.

- Management of Risk (M_o_R). Available from Office of Government Commerce (OGC): http://www.mor-officialsite.com/home/home.asp

Risk White Papers

Mosaic's risk White papers are:

- Risk Management: http://www.mosaicprojects.com.au/WhitePapers/WP1047_Risk_Management.pdf
- Types of Risk: http://www.mosaicprojects.com.au/WhitePapers/WP1057_Types_of_Risk.pdf
- Risk Assessment: http://www.mosaicprojects.com.au/WhitePapers/WP1015_Risk_Assessment.pdf
- Probability: http://www.mosaicprojects.com.au/WhitePapers/WP1037_Probability.pdf
- Our blog posts on risk are at: http://mosaicprojects.wordpress.com/category/project-controls/risk/

First published 13th August 2010, augmented and updated.

This White Paper is part of Mosaic's ***Project Knowledge Index***
to view and download a wide range of published papers and articles see:
http://www.mosaicprojects.com.au/PM-Knowledge_Index.html

First published: 13th August 2010 – extensively augmented and updated.