Project Risk Management Guideline

Version 3.3

Thursday, June 30, 2011

Document Ownership Information

Document Owner	ICT Policy Branch
Document Preparation	
Document Confidentiality	

Document Name and Version Control
(Circulated versions only)

Document Name & Location		www.services.nsw.gov.au	
Version	**Date**	**Author**	**Changes Included**
1.0 (First Release)	Sept 1997		First release based on drafts and feedback from reviewers.
3.0	Sept 2004		New template
3.1	Feb 2007		Updated template and references
3.2	March 2011	D Anspal	Updated references, bibliography and template. Removed GCIO references
3.3	June 2011	D Anspal	Changed contact details

Table of Contents

1 Using this guideline 4
2 Introduction 5
3 Objective and Scope 6
4 Concepts 7
5 Roles 10
6 Some Risks in Risk Management 11
7 Risk Management Process 12
8 Appendices 14
Appendix 1 - Risk Management Process 14
Appendix 2 - Some Risk Identification Checklists and Prompts 25
Appendix 3 – Notes on Quantitative Methods 27
Appendix 4 - Risk Management Plan Template 32
Appendix 5 - Definitions 35
Appendix 6 - References 39

1 Using this guideline

The objective of this guideline is to provide guidance to project teams and project stakeholders on the application of the standard risk management process to Information and Communications Technology Governance (ICT) projects and programs in the NSW Government. It is applicable to ICT projects and programs of all sizes and its principles and techniques are applicable to risk management for other programs, projects, plans and activities.

National standard AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines provides the generic framework for risk management. This framework is an iterative process of sequential steps. For users with little experience in risk management the standard provides an essential foundation to this guideline. Reference may also be made to:

- Agency Corporate Risk Management policies;
- TPP 09-05 : Internal Audit and Risk Management Policy for the NSW public sector by New South Wales Treasury;
- HB 327:2010 Communicating and Consulting about Risk;
- IEC/ISO 31010:2009 Risk Management – Risk Assessment Techniques;
- ISO Guide 73: 2009 Risk Management – Vocabulary;
- HB 436:2004 Risk Management Guidelines Companion to AS/NZS 4360:2004; and
- Well recognised project management methodology, such as PRINCE2, PMBOK.

This guideline does not provide a detailed definition of all the actions to be taken, or of the detailed risk management organisation for a project or program. These will vary according to the circumstances. It describes:

- The standard risk management process, highlighting some useful techniques; and
- What should occur to manage the risks that are associated with an ICT project or program.

This guideline was produced to promote an understanding of the requirements for successfully managing the risks associated with a project and its product's life cycle – from concept to eventual disposal. It provides information and advice useful to project teams and those concerned with ICT governance.

This guideline comprises 5 sections:

- This first part provides an introduction, concepts and roles, and outlines the risk management process.
- Appendix 1 provides commentary on each of the six steps in the risk management process and their application to project risk management, some readers may find it useful to consult AS/NZS ISO 31000:2009 at the same time.
- Appendix 2 provides some checklists and prompts that can be used to assist with risk identification (Step 2).
- Appendix 3 provides an introduction to quantitative methods for those unfamiliar with it.
- Appendix 4 provides a suggested template for a risk management plan, including a risk register.
- Appendix 5 provides a list of definitions.

2 Introduction

Managing risk is one of the major processes of corporate governance and all its aspects including ICT governance. Risk management is a core discipline that assists managers at all levels to make correct and informed decisions.

Risk management is a process for organised assessment and control of risks. It involves the identification, analysis and evaluation of the risks presented by the system being acquired and the activities to acquire it, and the development of cost-effective treatments for those risks. It applies to projects and programs of all sizes.

Risk management is one of the seven project processes identified by international standard ISO/IEC 15288:2008 *Systems engineering – System life cycle processes*. The other six processes are: Project Planning, Project Assessment and Control, Decision Management, Configuration Management, Information Management and Measurement. In addition enterprise processes include: Life Cycle Model Management, Infrastructure Management, Project Portfolio Management, Human Resource Management and Quality Management. ISO/IEC 15288:2008 provides the framework for current leading practice and failure to implement these processes is a risk that will jeopardise a project.

Risk management can be challenging because it requires thinking that may be seen as detrimental to a project. Good risk identification requires ‘negative thinking’ and looking for potential problems. This can be seen as at odds with the ‘can-do’ attitude often expected by senior management. However, looking for difficulties and then managing them so that there are ‘no surprises’ for senior management leads to successful projects and is a mark of mature governance. Ignoring risks or being ignorant of them leads to failure.

Effective risk management has costs. However, it is an overhead to prevent loss.

3 Objective and Scope

The objective of project risk management is to apply a systematic process to reduce cost-effectively the effects of uncertainties that compromise project or business objectives.

All projects have risks and cost-effective management of risk is essential if a project is to achieve its business outcomes. These typically include cost, schedule, quality and the fulfilment of functional and non-functional requirements. Risk management starts at the inception of a project. This means risk must be addressed when the project's scope and justification are documented in its business need proposal and in its initial business case. The risk management process comprises six steps, see Figure 2.

The scope of risks in projects is broad, and Appendix 2 provides checklists of matters that should be considered. The risks are not limited to matters in the life of the project to deliver a system to the project's customer. They include risks affecting the delivered system's operational life. These impact the system design and must be managed as part of the system engineering process.

4 Concepts

Risk management is more than just the management of project risks, it is also the management of the risks that the project may place on the business. For example, if a project replaces a key system that supports services to an agency's clients then non-delivery, or provision of a system that is difficult to use, could severely degrade the agency's operations and service delivery capabilities.

Risk management is an iterative process for identifying, analysing, evaluating, treating and monitoring risks. It is governed by a risk management plan and controlled via a risk register.

Effective risk management requires an investment of resources. Furthermore, risk management for a particular project cannot be efficiently addressed without an organisational context to provide policies and guidance. Therefore, a key goal for risk management is to cultivate support among those who do not have a direct business interest in the actions and resources needed to treat risks. Good governance requires an organisation to have documented and approved policies for risk management.

Risks are significant uncertainties about outcomes, the uncertainty is in two dimensions, the likelihood of the risk event occurring, and the extent of the consequences if it does. Different domains use different terms for risks. For example security tends to use 'threat' while occupational health and safety (OH&S) or environment uses 'hazard'. For projects it is usually convenient to refer to risk events. Whatever term is used it is always important to understand the sources of the risk event.

Risk events give rise to problems, some of which may be absorbed or accommodated, but others have impacts that affect project objectives. Naturally, there is seldom a one to one relationship.

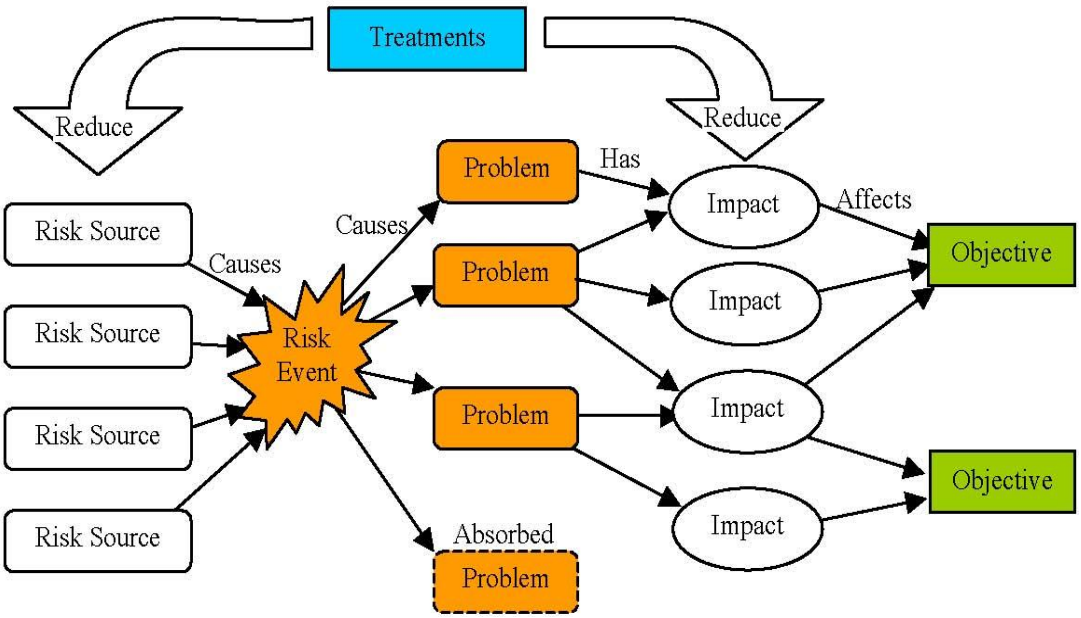

Figure 1: Risks have sources and impact objectives if untreated

The consequences of an uncertainty can be negative or positive. While it is usual to focus on the negative risks, positive risks cause opportunities not problems. Consideration of possible positive consequences enables projects to exploit them beneficially.

If a risk event occurs before it is treated then it is a problem that changes the current reality. It then has to be managed via treatments to reduce its impact or contingency plans, or new plans if it was unforeseen. An undesirable event that is a certainty in terms of its likelihood and consequences is also a problem, not a risk. It has to be managed as part of the normal project planning or replanning process. An issue is not necessarily a risk, it is a 'point of debate, discussion or dispute that requires resolution'. An issue may be either an uncertainty, its resolution means treating it as a risk, or a certainty in which case it is a problem to be actioned.

However, while a problem may be certain all its ramifications may be unclear. Risk management techniques may be applicable in selecting the optimum solution to the problem. This highlights the important role of risk management techniques in system engineering.

The risks associated with a project can be:

- Inherent, which result from the nature of the project objectives and scope;
- Acquired, which result from the selected organisation, approach, technology, methods, tools, techniques, skills and experience that are applied to the project; or
- Contextual, which result from events, circumstances or inter-relationships outside or across the project or system boundary and impact aspects of the project.

Inherent risks are more difficult to reduce but can be managed, often through a change in the nature or scope of the project. For example, a project may have a high implementation risk due to the wide scope of the new system. Breaking the project into increments that deliver successively more operational capacity may significantly reduce this risk, providing the system level architectural design is right. And this proviso is, of course, an acquired risk.

It is normally neither feasible nor necessary to eliminate all the risks associated with a project. However, once they are identified and documented the risks can be cost-effectively treated. Effective management of risk will usually require a balance to be struck between the:

- Scope and quality of the project's deliverables and the extent to which they satisfy the needs of the business;
- Time-scale for the project; and
- Cost of the project.

Effective management of project risks requires:

- **Commitment at all levels**. The commitment to managing a project's risks must start with the agency's senior management and sponsor, and continue through all participants and stakeholders in the project.
- **Communication and consultation.** The project must maintain contact with their internal and external stakeholders at every stage of the risk management process and concerning the process as a whole. Risks are prone to varying perceptions and it is important to reflect and reconcile these.
- **Effective system engineering and project management**. The project must ensure that there are plans and processes for managing the project's risks. The project's management team should, through participation in similar projects, have a good understanding of the risks that the project may face and of appropriate methods for managing those risks.
- **Risk ownership.** Each identified risk must be assigned to the person, role, team, unit or agency best able to manage it in terms of their responsibilities. They must have the overall responsibility and authority for managing the risk.
- **A continuous approach.** Risk management is a continuous process throughout all stages of a project. The project team must constantly monitor the project's risks to assess the effectiveness of the risk management measures, to identify any new or changing risks, and develop revised risk treatments as appropriate.
- **A partnership approach.** The project stakeholders, including project team (both in-house and contractor), the business and contextual influencers such as related projects must work closely together to identify and manage risks.
- **An appropriate risk management process.** The use of proven methods can significantly increase the effectiveness of the risk management process. Appropriate methods and techniques, used by experienced managers and team members, will guide the identification and analysis of risks and will assist with the development of effective risk treatments.

5 Roles

The key roles in risk management, and their major responsibilities are:

Senior management, who must promulgate organisational risk management policy, actively support the risk management actions required for the project and ensure that all project stakeholders and participants support those actions. The extent of their routine involvement in a particular project will depend on the project's characteristics.

Sponsor, is responsible for:

- ensuring that adequate resources are available to manage the project's risks;
- ensuring there is active participation in the risk management process by a wide cross section of stakeholders in the project;
- ensuring that risks that affect the project from outside the project's boundary are managed; and
- monitoring and reporting the progress and effectiveness of the risk treatments.

Project Manager/Director, heads the project team and is assigned the authority and responsibility for meeting the project objectives including the overall management of risks within the project.

Risk Owners, have the overall responsibility and authority for treating the identified risks. Within the project team they would be work package managers but risks to the in-service system may belong to the business unit owning the system. Risk owners must have the resources necessary to treat their risks. Risk owners are also assigned to monitor risks that are not being treated.

Risk Manager, the person in the project with the overall responsibility, accountability and authority for ensuring that the risk management process is applied effectively, including:

- driving and managing all aspects of the risk management process;
- ensuring all risks have an appropriate owner;
- maintaining the risk register, a template is included at Appendix 4;
- ensuring appropriately frequent risk reviews to identify new or changing risks;
- continually monitoring the cost-effectiveness and practicability of the risk treatments;
- preparation of regular risk reports in accordance with the risk management plan; and
- seeking and implementing continuous improvement to the risk management process and sharing lessons with other projects and stakeholders.

Business Representatives and Business Owner, must assist with the identification, analysis and evaluation of risks and support the implementation of the selected risk treatments.

Project Team Members, are responsible for:

- assisting with the identification, analysis and evaluation of risks;
- assisting with the development of risk treatments; and
- risk management activities as set out in the risk treatments.

6 Some Risks in Risk Management

There is a risk that the following might impact the project's objectives:

- inadequate resources causing ineffectively managed risks;
- risk management costs excluded from the business case causing their exclusion from cost benefit analysis which impacts the project's viability;
- a project without a risk reserve budget causing risk treatments to be unaffordable;
- the wrong mix of skills and experience in a project team causing inadequate risk management;
- risk treatments are inadequately integrated with the other project plans causing unidentified interdependencies and resource conflicts;
- late discovery of a risk causing increased cost and complexity for managing that risk;
- as a project finds more risks it abandons formal risk management causing major new risks not being identified;
- there is optimism bias causing missing, ignoring or inadequately treating risks;
- risks change during a project causing planned treatments to become inappropriate;
- risk treatments fail causing planned treatments to be unacceptably ineffective;
- risk treatments causing secondary risks;
- inappropriate risk management methods and techniques causing ineffective or inefficient risk treatments; or
- security during a project may be compromised causing project plans to be altered.

7 Risk Management Process

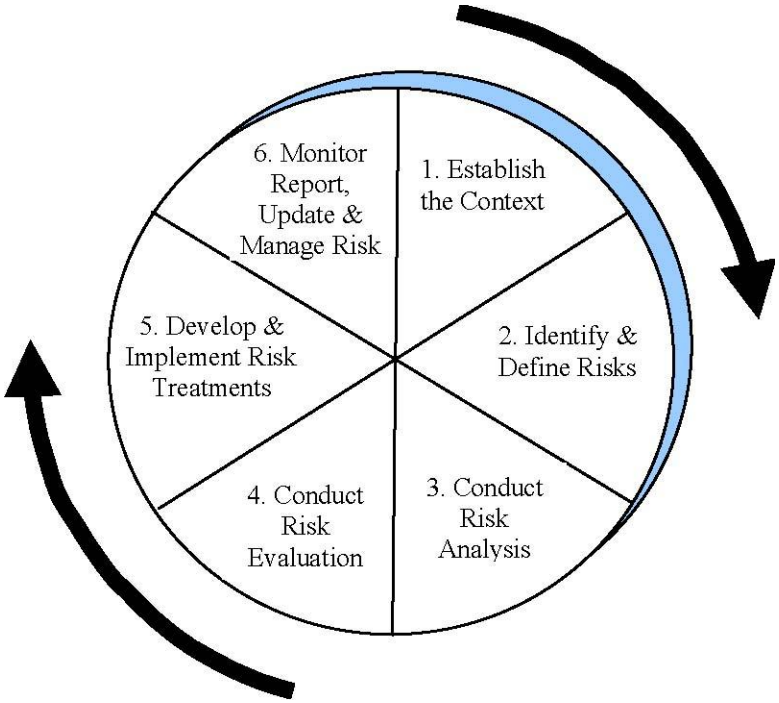

Figure 2: There are six major steps in Risk Management

As shown in Figure 2, there are six major steps in risk management. Steps 2 – 6 are not one-off events and are repeated throughout the project. Steps 2 – 4 are collectively called assessment.

1. **Establish the context**. Define and identify the organisation and project environments, characteristics, dependencies and stakeholders, their goals and objectives, and the scope and boundaries of the specific risk management process. Develop criteria against which risks are evaluated and identify the structure for risk management. Ensure all assumptions are recorded in the Project Charter or Assumptions List. When the context has been established then the risk management plan can be prepared.
2. **Identify and define risks**. The project's risks are best identified through a collaborative approach involving a wide cross section of stakeholders in the project and recorded in the project's risk register. At the start of each project phase, the risks associated with that phase are formally identified through a similar process. All conceivable risks, including 'show stoppers', must be considered. Ensure any certainties are identified as problems and addressed in the project processes.
3. **Conduct risk analysis.** An analysis of the risks is conducted to determine their causes, and estimate their probability and consequences.
4. **Conduct risk evaluation.** The risks are considered and prioritised according to their potential impact on the business and the project, and each risk is assessed to determine its level of acceptability. The risk register is updated with the outcomes of the risk analysis and assessment process and identifies the risks that require management and assigns owners to them.
5. **Develop and implement risk treatments.** Risk treatments are developed to cost-effectively reduce, contain and control project risk. Formal risk management reporting mechanisms are also defined.

6. **Monitor, report, update and manage risks.** As risks change during the project, the risk profile is continuously monitored, reviewed and updated. New risks may be identified as more information becomes available and existing risks may be eliminated through the effectiveness of the risk treatments.

Appendix 1 provides more detailed information about each of these six steps in the risk management process with further information located in AS/NZS ISO 31000:2009 and HB 436:2004.

Summary

Risk management is an essential component in the successful management of any project, whatever its size. It is a process that must start from the inception of the project and continue until the project is completed and its expected benefits realised.

Risk management is a process that is used throughout a project and its products' life cycles. It is useable by all activities in a project.

Risk management must be focussed on the areas of highest risk within the project with continual monitoring of other areas of the project to identify any new or changing risks.

The success of a project's risk management strategies is dependent on the:

- commitment of the sponsor and senior management to the risk management process;
- skills and experience of the project team in the assessment of risks and the development of effective risk treatments;
- project team, the business and other stakeholders working closely together to identify and manage all risks affecting the project;
- use of an appropriate risk management process, methods and techniques continuously throughout the project; and
- regular reporting of performance against risk treatments, with this reporting provided by the project team and through appropriate independent quality assurance processes.

8 Appendices

Appendix 1 - Risk Management Process

Step 1. Establish the context

Purpose

The purpose of this step is to establish, for the project or program, the parameters for risk management and the criteria against which risks will be assessed.

Commentary

The first step is to establish the strategic, organisational and risk management context in which the rest of the risk management process will occur. The starting point for this is the organisation's enterprise level risk management policies and processes.

The strategic and organisational context is the relationship between the organisation and its environment, characteristics and functions. Stakeholders must be identified. Risk management takes place in this wider context. Understanding this helps to identify and assess risks and plan acceptable treatments.

The specific project risk management context must also be established. This identifies the boundaries of the risk management activities and the necessary risk interfaces with other projects and organisations.

Risk management must be appropriate to the overall risk exposure. One approach for smaller projects is to undertake a 'flash' assessment to identify any significant risks. The results of this will determine the subsequent scope of risk management activity. For some projects regular independent external reviews may be appropriate as a strategic risk treatment.

The project context leads to the appropriate level of risk management effort and initiates the risk management plan. A template for a risk management plan is provided at Appendix 4.

Outputs

Initial version of the risk management plan including the risk management policy for the project or program.

Summary of key elements in establishing the risk context for a project:

- Establish the strategic context;
- Establish the organisational context;
- Establish the risk management context; and
- Prepare the initial version of the risk management plan.

Step 2 Identify and define Risks

Purpose

The purpose of risk identification is to identify and define the positive and negative risks that may affect the project or program.

Commentary

The identification of the risks associated with a project should start when the concept for the project is first developed

Risks are uncertainties affecting the achievement of the project's objectives. It therefore follows that risks cannot be fully identified if objectives are unclear. The project's business case must identify all known risks that may affect the complete life cycle from concept to eventual disposal of the system delivered by the project. The project's cost benefit analysis must consider the estimated life cycle costs for the management of those risks from initiation onwards. At this stage the project's risk register (part of the risk management plan) must be opened, and for larger projects an assumptions list should also be created.

Unidentified risks cannot be managed. Effective risk identification must overcome barriers such as a 'can-do' or 'she'll be right' attitude; the unthinkable must be considered and not seen as 'undermining' or 'negative thinking'. A typical failing in risk identification is to focus on the easy and minor problems and ignore the potential 'show-stoppers'. One effective approach to catastrophic risks is to start with the catastrophe and work back to its sources.

Risk management is a continuous process, it is an inherent component of analysis, design, implementation and in-service support planning of any ICT system. Risks will change during these activities; risk estimates will be refined, some risks will disappear and new ones will emerge.

Risk management is an integral part of requirements engineering. This means applying it during analysis, synthesis, trade-offs and architectural design during the system engineering processes and to software architectural and detailed designs. Established techniques such as Event Trees, Fault Trees, Master Logic Diagrams, Event Sequence Diagrams, Reliability Block Diagrams, Failure Modes and Effects Analysis, and Failure Modes and Effects Criticality may be applicable.

In addition to embedding risk management into all aspects of a project, the risk register should be periodically reviewed as a formal activity established by the risk management plan. This should be at milestones, particularly at the start of stages, but for larger and longer projects should be periodic, and no less frequent than every two months.

Effective methods of risk identification include:

- Brainstorming, with a facilitator and range of stakeholders;
- Interviews with stakeholders;
- Scenario, business analysis and event tree modelling;
- Dependency modelling;
- Experience from other projects, metrics and published data for norms;
- Reviewing project information, including plans, analysis and designs; and
- Checklists.

Many risks are products of estimates, which are inherently uncertain. One way of identifying risks is to recognise those matters where two or more people, competent in the matter, could give different answers.

Stakeholders include the business owner, business managers from key functional and business areas, project team members, relevant specialists, operators, users and clients. The last are particularly important because well managed projects often deliver 'solutions' that are not fully adopted by their ultimate users. This means the project at least partially fails.

Many common risk sources can be identified at the start of a project and treated before they have any significant impact. Risk identification requires a broad and forward-looking view, experience, and an element of lateral thinking. Some checklists for risk identification are in Appendix 2. In some domains consideration of vulnerabilities is another useful approach to identifying risks. The possibility of risk treatments failing is itself a risk that has to be considered.

Identified risks should be meaningfully expressed, the preferred form of expressing a risk is – '*There is a Risk that [Risk Source] cause [Consequences] that impacts [Project Specific Objectives]*.'

It is also important to record relationships and commonalities between risks to facilitate their subsequent management and identify consequences that may compound or chain. For example one risk event may have several impacts, one impact may have knock-on effects on others and two or more risks may disproportionately increase a shared impact. Risks that affect the key project managed elements of cost, schedule and scope/quality (fulfilling functional and non-functional requirements) should also be clearly identified.

Output

Identified risks are recorded in the risk register.

Summary of the key elements in the identification of a project's risks

- Identify risks in the initial and revised business cases;
- Review risks throughout the project in accordance with the risk management plan;
- Document identified risks in the risk register;
- Consider all risk sources;
- Encourage wide participation; and
- Use a formal process and appropriate methods and techniques.

Step 3 Conduct risk analysis

Purpose

The purpose of risk analysis is to consider all identified or changed risks to produce valid input for decision making in the evaluation step.

Commentary

The analysis of the risks associated with a project requires high levels of participation by key representatives of the business, project team and other stakeholders.

Risk analysis can be undertaken using similar methods as used for risk identification. Risk analysis is also a continuous process in the same way that risk identification is and the two may often be combined, in a structured way, into one activity.

Project or program risks are analysed to identify:

- estimated likelihood that the risk will occur (preferably probability using quantitative methods);
- estimated consequences of the risk occurring in terms of its cost, schedule, 'quality' and other impacts on the project objectives including its products;
- the most appropriate risk owner; and
- potential impact of the risk on third parties such as other projects and organisations.

It can also be useful at this stage of the analysis to conduct an initial high level assessment of whether the risk should be managed. There are four cases where a risk may not need managing by a project:

- the likelihood of it happening is extremely small;
- the consequences make the project irrelevant;
- the consequences are insignificant and require no treatment; or
- the risk belongs outside the project, in this case the outside owners must formally take responsibility for it.

Wherever possible, the consequences of each risk should be valued. This is the risk exposure. At its simplest risk exposure = likelihood × consequence value. This is difficult to represent meaningfully using qualitative values such as 'high' and 'low', although these can be assigned numeric values to provide an interval scale. However, a more powerful quantification technique is to apply probabilities in techniques such as Monte-Carlo analysis and Bayesian analysis. Appendix 3 provides an overview of quantitative methods for assigning risk value.

Where the consequences cannot be quantified they are normally qualitatively estimated on a scale from low to high or similar. A qualitative approach to both likelihood and consequences may be the only option at the very earliest stages of a project, but should migrate to quantitative as soon as possible. Qualitative estimates should use the 'most likely' (ie not best or worst case) criterion for rating the likelihood and consequences of a risk. Examples of techniques using qualitative analysis include; Delphi technique, Cause and Effect analysis and Sneak Analysis.

IEC/ISO 31010:2009 provides guidance on the selection and application of systematic techniques for risk assessment.

When considering the likelihood of a risk that is outside the project schedule, a time-period usually needs to be adopted. Typically the product's expected life but possibly some term such as 5 years, whole-life cost time frame or the period used for benefits realisation. In

some instances, particularly ICT security, it may be appropriate to consider vulnerability to a risk as part of its probability, including representing vulnerability as a risk source.

When analysing risks it is important to document the information and assumptions underpinning the analysis, including the interdependencies between risks. This facilitates subsequent reviews and assessment changes.

Outputs

Estimates of the likelihood and consequences of risks and identification of the risk owners documented in the risk register.

Summary of the key elements in the analysis of a project's risks:

- Estimate the likelihood and consequences of each risk and the resultant risk exposure;
- Identify the most appropriate risk owner for each risk and assign the risk to them; and
- Document the outcome of risk analysis in the risk register.

Step 4. Conduct Risk Evaluation

Purpose

The purpose of risk evaluation is to decide which risks need treatment and their priorities.

Commentary

Once an analysis or review has been made of the risks associated with a project, the risks are evaluated to determine their treatment. The first action is to sort the analysed risks by classifying them as one of:

- **Accepted Risks**: risks that are currently acceptable and do not require treatment, but will be kept under review;
- **Rejected Risks**: risks that are considered non-existent after analysis or of no significance; or
- **Significant Risks** to be treated: these may need prioritisation.

Classification and prioritisation will be against risk criteria in the light of contexts and policies established in the risk management plan. It is important to remember that one risk source may have several consequences, direct or chained, and that there will be inter-relationships between risks. These will affect the significance of risk sources and their impacts.

Evaluation should also consider the sensitivity of the estimates to errors. This is significantly less of an issue when estimates have the form of a probability distribution because quantitative methods facilitate it.

Optimism bias is another consideration reflecting a human tendency to optimism. Quantitative methods can reduce this bias, which can be significant when project team members make the estimates. Other solutions include applying to estimates standard ‘multipliers’ derived from experience with similar projects or ensuring a process of rigorous independent review of risk identification and analysis.

In some instances it may be necessary to develop contingency plans:

- if the risk eventuates;
- when a critical decision point is reached without effective treatments being found; or
- when there is a likelihood that an effective risk treatment will not be found.

When a risk has not been treated in a way that entirely eliminates it, then indicators of the risk eventuating may need to be identified. Manifestation of the indicators means that the likelihood of the risk is increasing and contingency plans may need to be executed.

If risks are positive then treatments should endeavour to make them more likely to occur or enhance their beneficial impact.

Treatments may have secondary risks, which must be analysed and evaluated. This may occur where treatment involves re-work or additional work that affects cost, schedule, performance, scope or quality.

Accepted risks require a risk owner who is responsible for reviewing and monitoring them and reporting any changes that affect their likelihood or consequences.

In some instances a risk can be so severe that the viability of the project may need to be reassessed. These risks must be highlighted and formally considered by the sponsor and, depending on the scale of the project and agency procedures, senior management up to chief executive officer (CEO) level to decide the appropriate action.

Outputs

The outcome of the risk evaluation is an updated risk register. This is reviewed by the sponsor. Any changes to risk must be fully reflected in approved revisions of the business case.

Summary of the key elements in the evaluation of a project's risks:

- Classify the risks;
- Prioritise significant risks; and
- Update the risk register

Step 5 Develop and implement risk treatments

Purpose

The purpose of this step is to identify, assess and implement measures to modify risks.

Commentary

The risk owners prepare treatments for the risks assigned to them. Risk owners may be members of the project team, business or other managers elsewhere in the agency, participating agencies or other stakeholder bodies. They will require an appropriate allocation of resources for their task(s), which may require negotiation by the sponsor depending on their relationship to the project.

Treatments will either reduce the risk's likelihood or consequences or both. Preparation of treatments usually requires inputs from stakeholders and coordination with the project manager and risk manager. If there is an unacceptable risk of treatment failing (or not being found) or when a risk may reach an unacceptable level then a contingency plan must be developed. Secondary risks may be a consequence of risk treatment and may necessitate their own treatment or contingency plans.

Risk treatment has both tangible and intangible costs and care must be taken to ensure that the cost of treating a risk does not exceed its anticipated impact. This means that treatments must be costed, cost-effective and practical.

In some cases risk treatments will be embedded in the project. For example the risk of project estimating errors is best handled quantitatively and treated by appropriate allowance in the project schedule and cost plan. However, there is then a risk of self-fulfilling worst case prophecies, which have to be managed by setting 'stretch' targets and carefully selected 'must achieve' milestones. This is best done in a staged project design.

The major approaches for treating negative risks are:

- **Reduce likelihood**, where the project or its environment is changed to reduce the probability of a risk occurring;
- **Reduce consequences**, where action is taken to minimise the impact of a risk if it occurs. Treatment includes contingency planning that should address significant risk areas where preventive action is either unavailable or the cost of prevention is prohibitive;
- **Avoid risk**, by not proceeding with the aspect that may suffer the risk event; or
- **Risk transfer**, where the responsibility for a risk is transferred to another party such as a supplier or insurer.

A range of treatments may be available for each risk and the risk owner must assess each option. Risk treatments may be reflected in project planning and can affect cost and schedule. However, early action may permit them to be undertaken as modified future activities without cost or schedule impacts. Risks that are identified later in a project's implementation stage are more likely to have a significant impact on costs and schedule. It may be necessary to update the project's cost benefit analysis to reflect the anticipated costs of the risk treatments.

For each risk that is to be treated the risk treatments should identify:

- the risk owner responsible for treating the risk;
- any relationships between risks;
- indicators of the risk increasing or decreasing;
- the approach to be used to treat the risk;

- assessment of the likelihood of the treatment being effective and mechanisms for measuring the effectiveness of the risk treatments;
- if necessary, a contingency plan, including an implementation decision point, if the risk treatment is insufficiently effective;
- the budget for the treatment; and
- if appropriate a time-scale for the completion of the risk treatment.

The risk treatments must be integrated with the overall project plan. This will ensure that any dependencies or potential resource conflicts between project tasks and risk treatments are identified and resolved. Where appropriate, the risk treatments should be linked to other business plans within the agency such as the corporate risk management plan.

Formal risk treatment reporting mechanisms should also be developed. Risk treatment must by monitored by the risk manager and incorporated with the regular project progress reporting to the project's sponsor and agency management as applicable.

Outputs

Planned treatment action for all risks that are not accepted and the risk register and project plans appropriately updated.

Summary of the key elements in the development and implementation of risk treatments:

- Identify risk treatments options;
- Assess each treatment including the need for contingency plans;
- Integrate treatments into the project plans;
- Document and cost risk treatments; and
- Develop risk reporting mechanisms to the sponsor and other stakeholders in accordance with agency delegations and procedures.

Step 6 Monitoring, reporting, updating and managing risks

Purpose

The purpose of this step is to monitor and report on the effectiveness of all steps in the risk management process.

Commentary

All projects should have a risk manager role. The person with this role has overall responsibility and authority for ensuring that the risk management process operates effectively in accordance with the project plans including the risk management plan. This role should also seek continuous improvement to the project's risk management processes and enable other projects to learn from their experience. However, this role is not the owner of all risks.

It is at least highly desirable that when a contractor is undertaking any part of the work then their risk management is appropriately integrated with that of the customer agency. This may be achieved through a joint register of risks and its regular review, although both parties may have additional risks in their own registers. Of course a shared list of risks does not mean a shared responsibility for managing them. The extent of a contractor's risk reporting to the customer will depend on what is agreed in the contract.

As a project progresses its risks will change due to unforeseen factors. These include new or revised business requirements, changes in legislation or a supplier no longer able to provide a particular product. It is therefore essential that the project's risks are continuously monitored, regularly reviewed and updated. The frequency of these reviews depends on the duration of the project but should be a mixture of periodic and event based reviews. On larger projects they should be no less frequent than every two months.

Particular care must be taken to reassess risks to a project when:

- a new stage of the project starts;
- there is a significant change in the scope or approach of the project; or
- a substantial change occurs in the project's stakeholders or environment such as a new sponsor or project manager.

Review of risks may lead to the:

- identification of new risks;
- elimination of risks that no longer apply; and
- reclassification of existing risks where the estimated likelihood or impact has either increased or reduced.

Care must be taken to ensure that project management attention is not overly focussed on areas that were initially assessed to be high risk. This may result in a failure to detect the emergence of new risks or the escalation of existing risks in other areas.

The assessment of any newly identified or changed risks is conducted in the same manner as described in the earlier sections of this guideline. The outcome of this process is used to update the risk register. The risk treatments are also updated or new ones created to reflect the new or revised risks treatments that are to be adopted for the project. Ensure that changes to risk are fully reflected in any updates of the business case provided for gateway reviews.

Formal risk reporting arrangements to the appropriate organisational level must be established. Risk reports must highlight changed risks and contain relevant and concise information that can be efficiently assimilated by the reports' audience.

Risk monitoring and reporting needs to address two matters:

- progress in the treatment of significant identified risks, including any indications that treatments may fail; and
- monitoring the project for indicators of other risks, that may or may not have been identified, emerging or growing. This involves analysis of project metrics, and when the risk has been identified its indicators should be recorded in the risk register.

The following table is an example set of types of project metrics:

Area	Measurement Category	Indicator
Schedule	Milestones	Milestone Achievement
	Product Completion	Requirements Fulfilled Earned Value Graph & Indices
Resources and Cost	Personnel	Staffing Profile
	Financial Performance	Earned Value Graph and Indices
Complexity & Stability	Physical Size & Stability	Components, Lines of Code Interfaces
	Functional Size & Stability	Requirements Fulfilled
		Requirements Changed
Product Quality	Functional Correctness	Defect Profile
		Software Design Coverage
	Test Coverage	Test Coverage
		Execution Failure Rate
Process Performance	Process Efficiency	Productivity
	Process Effectiveness	Defect Containment
Configuration Management	Amount of Change	Change Requests
Interfaces		Percentage of Interfaces Defined

Outputs

Updated risk register and reports as required by the risk management plan.

Summary of key elements in monitoring and updating a project's risk profile:

- There must be an overall risk manager;
- Regularly review the risks;
- Monitor the emergence of new or changing risks;
- Update the risk treatments;
- Maintain the risk register; and
- Risk reports to appropriate recipients including the sponsor and management in accordance with agency delegations and procedures.

Appendix 2 - Some Risk Identification Checklists and Prompts

Broad categories of risk provide a useful prompt-list of possible problems to both the project and the delivered system. These include:

- Timescale;
- Financial;
- Skills and resources;
- Technical and technological;
- Business impact;
- Security and safety (including safety critical where a malfunction may result in loss of life);
- Stakeholder interests (including end-users, suppliers, operators, affected parties and business owners); and
- Environment (including legal, commercial, political, social, economic, natural, ethical, competitive, infrastructure, information availability, reputational).

DeMarco & Lister have identified 5 core risks common to all software projects, as follows:

1. **Schedule Flaw:** basically inaccurate estimating of cost and schedule, a consequence of wrongly estimating the amount of work.
2. **Requirement Inflation:** sometimes diagnosed as ‘changing minds’, ‘re-interpretation’ or ‘scope creep’. It also reflects the unavoidable reality of a continuously evolving business environment, which has to be accommodated.
3. **Turnover:** staff depart and have to be replaced, and it takes time to get replacement staff ‘up to speed’.
4. **Specification Breakdown:** this is a binary risk, it either happens or it does not, and if it does it is a potential catastrophe. Its root cause is the inability of stakeholders to agree, sometimes after ‘papering-over’ disagreement by agreeing to an ambiguous requirement.
5. **Under Performance:** developers and development teams may be better or worse than average. Larger teams are more likely to be average and new teams below average.

Another checklist of project and agency management risk sources includes:

Requirements & Analysis	Maturity of functional and non-functional requirements. Quality of analysis and synthesis. Test, evaluation & acceptance processes. Development and maintenance of the related project documents.
Resources	The sufficiency of funding to cover acquisition including project support activities. Dependency on the supply of goods and services.
Project Processes	Maturity of the full range of processes, tools and training to support them. Maturity of the skill and experience available in agency project management and support activities.
Technical	Current maturity of relevant technologies, integration and interoperability matters, engineering processes, skills. Ill-defined areas of technical specification, discrepancies between acceptance tests and the operating environment. Safety critical and security aspects.
Sustainability	Relating to the sustainability and supportability of the production system throughout its expected operational life.
Training	Relating to the skills, tools, training and development required to provide competent users and support staff throughout its expected operational life.
Government Environment	Restructuring consequences for requirements and resources. Legislative changes affecting requirements and operating rules. Compatibility with existing legislation.
Commercial	Take-overs, relocation of contractors, industrial relations, changes in business direction. Contractors' resourcing, financial, legal. Management stability of contractors and sub-contractors.
Quality and Capability Maturity	The customer's and contractors' Quality Assurance status. The Capability Maturity of customer and contractor organisations in the process dimensions of Process Management, Project Management, Engineering and Support.

Other lists of risks can also be found in HB 436:2004 as well as the Software Engineering Institute's report *A Proposed Taxonomy for Software Development Risks for High-Performance Computing (HPC) Scientific/Engineering Applications* which provides a comprehensive taxonomy of software implementation risks.

Appendix 3 – Notes on Quantitative Methods

Introduction

Risk analysis has used mostly qualitative methods, for example likelihood being ‘High’, ‘Medium’ or ‘Low’ and consequences being ‘Moderate’, ‘Severe’ or ‘Catastrophic’, these are ordinal scales. There are two problems with this approach, first their meaning can be very widely interpreted and second you cannot do much with them except to have arbitrary rules about combining them and taking this as an indicator of the overall significance of the risk. This is useful but of limited business utility. You can convert them to interval scales by substituting numbers for the names. This has some worth because you can use the numbers mathematically, but their interval scale limits their validity.

Quantitative methods are now becoming common and are sometimes called probabilistic risk assessment. Their attraction is that they use ratio scales so numbers can be directly applied to other numeric data such as dollars, days and lines of code. This means that appropriately used quantitative methods enable some risks to be costed with a useful degree of assurance.

Quantitative methods are used in risk management to calculate risk exposure where, in simple terms, risk exposure = likelihood × consequence value. However, both likelihood and consequence values are uncertain estimates and this means that they are actually a range of possible values, most obviously because different estimators would almost certainly give them different values. Each value in the range has an associated probability. Quantitative methods should be used in preference to qualitative methods when possible and appropriate.

Likelihood and Consequence

Generally, consequences are either binary or continuous; a set of discrete consequences is very unlikely. A binary consequence is ‘all or nothing’, there is a likelihood of it happening but if it does then there is only one consequence. This contrasts with continuous consequences where there is a continuous range of possible consequence values, as well as a range of estimates for their likelihood.

That said, some risks are certainties in terms of their likelihood although their consequences will be a continuous range of values. In projects it is a certainty that any particular single value estimate will be wrong, for example the cost of a work package, the time it will take, the number of lines of code or the value of each tangible benefit of the project. In reality the estimated consequences are a range of possible values, but it is seldom the case that all the values in the range are equally likely.

Probability Distributions

Two forms of graph represent ranges of values and their associated likelihoods: probability density functions and cumulative distribution functions. Both use the same data, probabilities on the vertical axis and the range of values on the horizontal. The best known probability density function is the ‘normal distribution’ represented by a ‘bell curve’. This is a good representation of naturally occurring phenomena but seldom representative of the range of estimates for such things as project cost or time, which may be skewed by such things as optimism and non-linear relationships.

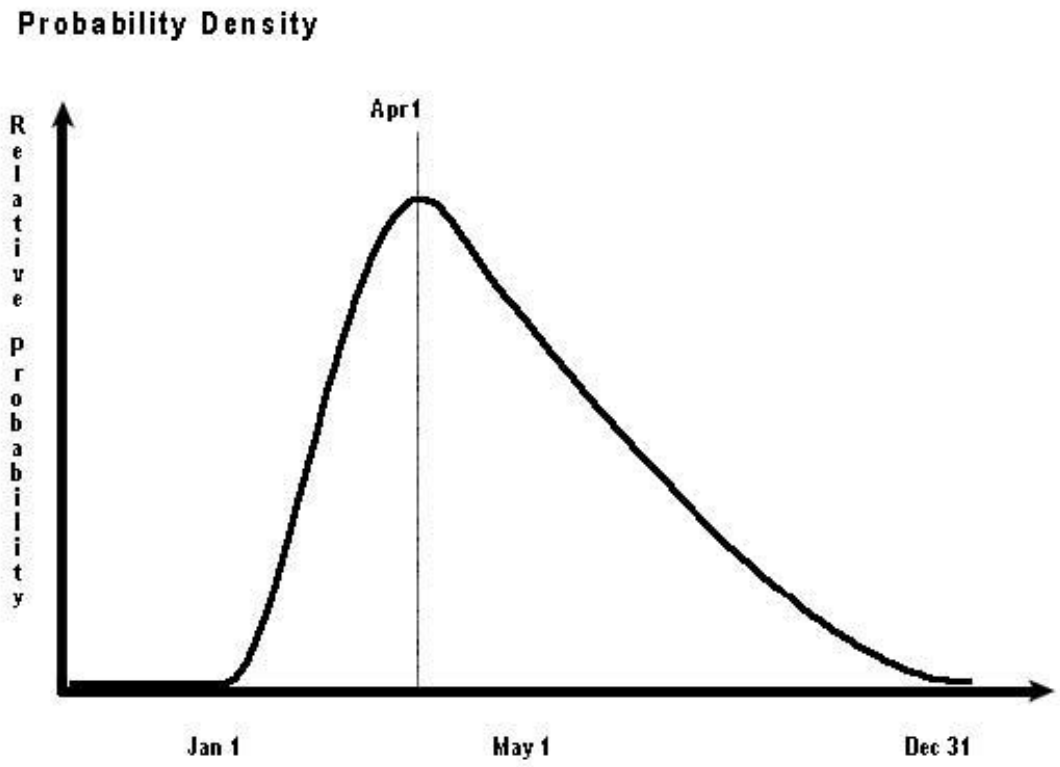

Figure 3: Probability Density

Probabilities are usually expressed as being in the range 0 to 1, although some people prefer to call this 0% to 100% chance. The probability density enables the probability of any particular value to be read from the graph. Being a density it also means that the area under the curve totals 1 or 100%, which means that to find the value for a particular probability you have to estimate the area under the curve that is covered by it. This is not always easy.

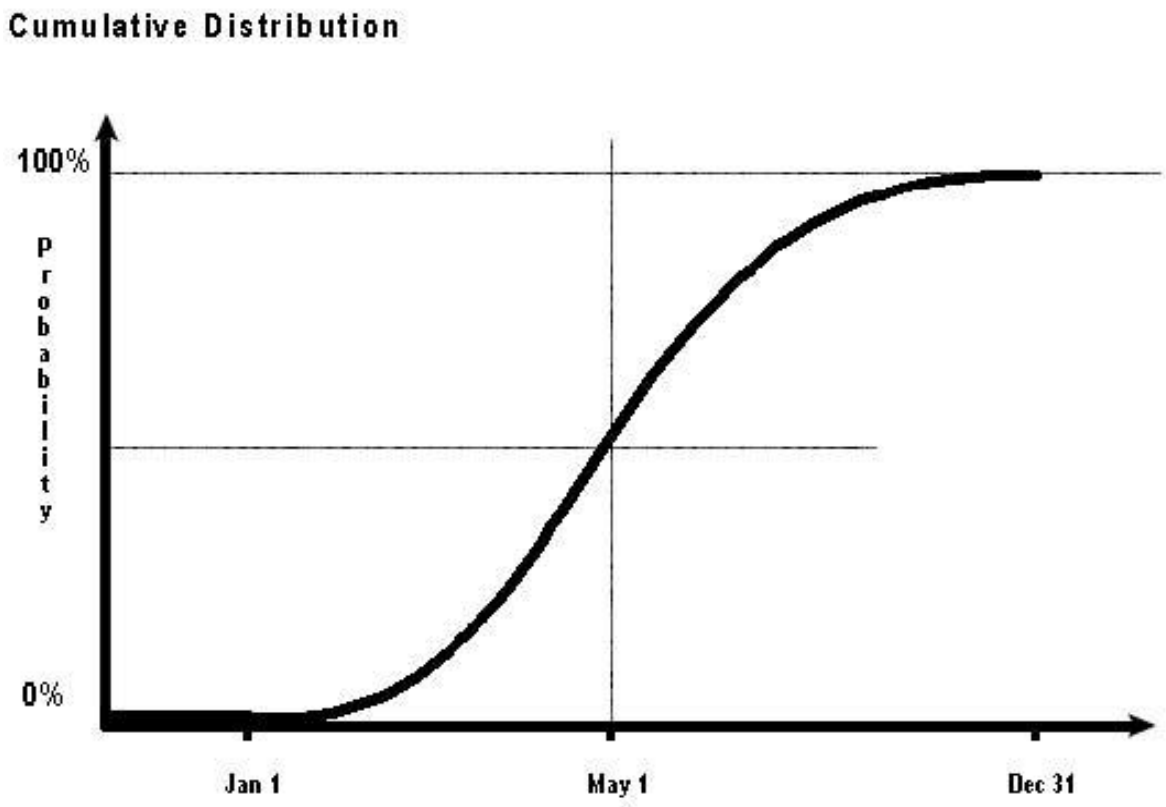

Figure 4: Cumulative Density

The cumulative distribution provides a different view, it enables the value for a particular probability to be easily read from the graph. Using these two graphs there are several important points:

- The peak of the probability density curve is the most likely value, the statistical mode.
- The 0.5 or 50% probability value on the cumulative distribution graph is the statistical mean.
- For right skewed distribution: Mode < Median < Mean
- For normal distribution: Mode = Median = Mean.
- For left skewed distribution: Mode > Median > Mean

Collecting metrics about planning estimates and actual outcomes enables organisations to develop empirical distribution models for the accuracy of their estimating. These can be applied to future estimates. This type of organisational capability is an indicator of capability maturity. However, although there are published data about project metrics, they may or may not be particularly applicable to a specific organisation.

An alternative is using a triangular, or '3-point', distribution, which is simple and usually provides an adequate approximation. This involves estimating the most likely value, the minimum value and the maximum value, although the last two are usually taken to represent 10% and 90% confidence levels. There are many distributions and some users prefer a Beta distribution that flattens the peak of the triangle in the probability density graph.

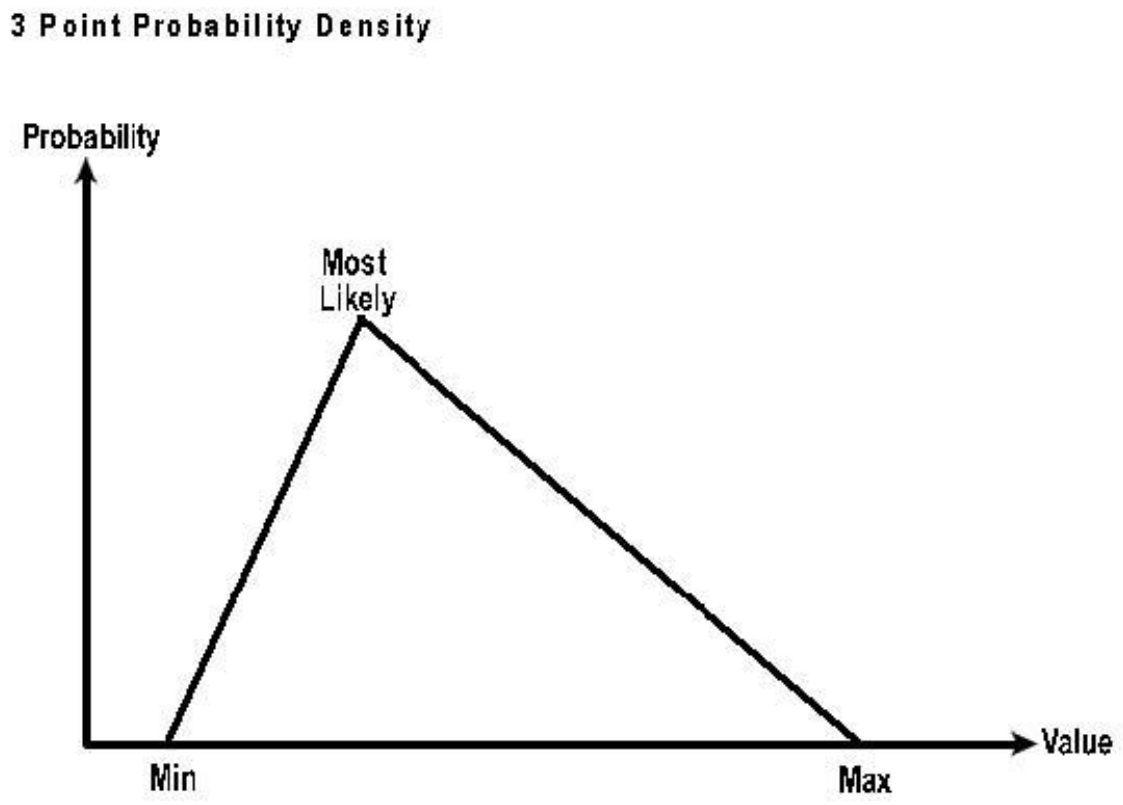

Figure 5: 3 Point Probability Density

Clearly, the wider the number of values in the range the lower the probability of the most likely, and this is affected by the units of measurement that are used. Working in dollars will give a wider range of values that working in thousands of dollars, and days a wider range than months. The probability of a task taking exactly 105 days is clearly less than it taking between 100 and 110 days.

Combining Estimated Values

Estimates often need to be combined, a project typically comprises several work packages each with varying time or cost estimates. Each has its range of possible values either side of the 'most likely'. Merely add up the numbers for the type of estimate (cost, time, etc) often not revealing whether they are optimistic, pessimistic or merely hopeful, is not good practice. They could be combined using calculus but the accepted technique is to use Monte Carlo simulation by computer.

A Monte Carlo simulation involves selecting random numbers in the range 0 to 1 (ie the spread of possible probabilities) in a way that mirrors the frequency of the probability in the probability distribution you are using. Using the cumulative data it then finds the value corresponding to the probability. This is done for two or more types of estimate (eg likelihood and consequence, several consequences or the likelihoods of several risk sources). The resulting values are then combined using the appropriate mathematical function. This process is repeated, typically several hundred times. The result is a new probability and cumulative distribution that provides the mean, mode and any other type of probable total for the combined values. Obviously the uncertain values being combined must have a mathematical relationship, for example cost derived from estimates of days and costs per day.

Monte Carlo simulation can be used to combine consequences (ie the values of several impacts of a single risk event), or the likelihoods of the sources for a risk event, or the

combination of likelihood and consequence of a risk event. For consequences the value will typically be measured in time or dollars For likelihood the value will be time.

The key point is that in the probability density graph the total area under the curve represents 1 (or 100%), in other words the maximum value represents the timeframe in which the risk event will occur. Often this will have a uniform distribution, for example it will occur once in 10 years, giving a probability of 0.1 in any year. Clearly there's no need to use Monte Carlo methods with this and the probability can be applied directly, either 0.1 per year or 0.3 for a 3 year period. However, some likelihoods are more complex. For example equipment is more likely to fail as it ages and some electronic equipment can have a high probability of failure early and late in its life, with very low in between, a 'bathtub' curve.

There is an increasing choice of risk management tools applying Monte Carlo simulation some fully integrated with project management applications such as Microsoft Project. However, 'stand-alone' spreadsheet tools are also very useful and are available as 'freeware'.

Appendix 4 - Risk Management Plan Template

Introduction

There is no generally recognised format for a risk management plan (RMP). In many projects a 'stand-alone' RMP would not be justified. Instead risk management matters would be included in the overall project plan, with a separate risk register. However, any plan for action, a work program, needs to address various matters. A RMP is a dynamic document and its initial version, excluding the risk register, is a product of the process of establishing the risk context. The most dynamic component is the risk register, which will be updated frequently.

Outline of a Risk Management Plan

1 Introduction

1.1 RMP Purpose

- To manage the actions to identify, assess and treat risks to the project objectives and its delivered system
- To create, maintain, action and report upon the risk register

1.2 Intended audience

- All those stakeholders actioning risk management.

2 Risk Management Policy

2.1 General

- In accordance with AS/NZS ISO 31000:2009 Risk Management – Principles and guidelines and as outlined in this guideline in the context of the project and participating organisation(s).
- Reference enterprise risk management policies and risk appetite

2.2 Risk Management Objectives

- Broadly, to identify and appropriately treat risks affecting project objectives.

2.3 Risk Criteria

- The criteria to be used in risk assessment

3 Risk Management Organisation

3.1 Roles and responsibilities

- Identify all roles that have responsibilities that include risk management and outline those responsibilities.

3.2 Resources

- Available for risk management, budget and control.

3.3 Structure

- Including relationships with stakeholders outside the project boundary.

4 Risk Assessment

4.1 Risk Identification and Definition

- Outline methods and activities to produce risk management deliverables in associated work packages

4.2 Risk Analysis

- Outline methods and activities to produce risk management deliverables in associated work packages

4.3 Risk Evaluation

- Outline methods and activities to produce risk management deliverables in associated work packages

5 Coordination

5.1 Risk Register

- Configuration control arrangements, probably different to remainder of RMP.

5.2 Risk Monitoring

- Arrangements for risk monitoring, including of accepted risks

5.3 Risk Reviews

- Frequency and arrangements for periodic, milestone related and other reviews

5.4 Risk Reporting

- Nature, frequency and recipients of risk management reports

5.5 Coordination with related projects

- If necessary

6 Risk Register

- The risk register is probably best handled as a separate document or database although it is part of the RMP
- Generally, each identified risk will need a page to itself, however a tabular summary is preferred to status reporting
- Each risk that is not rejected requires a treatment, including contingency arrangements if appropriate

Risk Register

Possible contents for a risk register are outlined below. Sometimes it may be appropriate to record treatments in a separate plan or schedule cross-referenced to the risk register:

Risk Identification and Definition

Unique Identifier	Risk Name
Originator	Date
Definition – in the form '*There is a Risk that [Risk Source] cause [Consequences] that impacts [Project Specific Objectives]*.'	
Explanation and amplification – including assessment of existing controls and their effectiveness	

Risk Analysis and Evaluation

Likelihood	Consequences – eg cost/ time/ function/ performance
Overall Risk Level	Priority
Proximity – when it might occur in the project	
Related Risks – sharing sources and or consequences, treatment failure	
Disposition – Reject/Accept/Treat	Date
Disposition – Reject/Accept/Treat	Date

Treatment

Risk Owner	Budget
Approach – Reduce likelihood/Reduce consequences/Avoid/Transfer	Effectiveness measure
Likelihood of residual risk	Consequences of residual risk
Overall residual risk level	Priority
Work item reference	Scheduled completion
Eventuating Indicator	Contingency Plan – required/ reference

Reviews and Monitoring

Risk Owner	Budget
Approach – Reduce likelihood/Reduce consequences/Avoid/Transfer	Effectiveness measure
Work item reference	Scheduled completion
Eventuating Indicator	Contingency Plan – required/reference
Risk Status	

Post Implementation Review

Risk Eventuated	Consequences

Appendix 5 - Definitions

Assumptions List	record of the assumptions embedded in the project plan. Assumptions that are not validated are potential **risks**.
Business Case [Wideman, modified]	document that justifies the need for the system to be delivered by a project, what the business changes will be and the resources required to deliver, operate and dispose of the system. It provides the basis for project funding and may undergo approved revisions during the project.
Business Owner	owner of the business case for the system to be delivered by the **project**. He/she represents the business needs of the agency or business unit and is the custodian of the user requirements.
Capability Maturity	organised characteristics of organisations in terms of their implementation and institutionalisation of best practices.
Client	may include end users and sponsors, potential end users or sponsors, potential providers or suppliers, current providers and suppliers, technical or functional experts and advisers, federal, state, local government, the organisation, other public service organisations, employees, unions or staff associations, industry bodies, local communities and society as a whole, special user groups.
Communication and consultation [ISO Guide 73:2009, definition 3.2.1]	continual and iterative processes that an organization conducts to provide, share or obtain information and to engage in dialogue with **stakeholders** regarding the management of **risk** NOTE 1 - The information can relate to the existence, nature, form, **likelihood**, significance, evaluation, acceptability and treatment of the management of risk. NOTE 2 Consultation is a two-way process of informed communication between an organization and its stakeholders on an issue prior to making a decision or determining a direction on that issue. Consultation is: - a process which impacts on a decision through influence rather than power; and - an input to decision making, not joint decision making.
Consequence [ISO Guide 73:2009, definition 3.6.1.3]	outcome of an **event** affecting objectives NOTE 1 - An event can lead to a range of consequences. NOTE 2 - A consequence can be certain or uncertain and can have positive or negative effects on objectives. NOTE 3 - Consequences can be expressed qualitatively or quantitatively. NOTE 4 – Initial consequences can escalate through knock-on effects.
Control [ISO Guide 73:2009, definition 3.8.1.1]	measure that is modifying **risk** NOTE 1 - Controls include any process, policy, device, practice, or other actions which modify risk. NOTE 2 – Controls may not always exert the intended or assumed modifying effect.
Establishing the Context [ISO Guide 73:2009, definition 3.3.1]	defining the external and internal parameters to be taken into account when managing risk, and setting the scope and **risk criteria** for the **risk management policy**
Event [ISO Guide 73:2009, definition 3.5.1.3]	occurrence or change of a particular set of circumstances NOTE 1 – An event can be one or more occurrences, and can have several causes. NOTE 2 – An event can consist of something not happening. NOTE 3 – An event can sometimes be referred to as an “incident” or “accident”. NOTE 4 – An event without **consequences** can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.
External Context [ISO Guide 73:2009, definition 3.3.1.1]	external environment in which the organization seeks to achieve its objectives NOTE External context can include: - the cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local; - key drivers and trends having impact on the objectives of the organization; and - relationships with, and perceptions and values of external **stakeholders**.
Hazard [ISO/IEC GUIDE 51:1999]	source of potential harm.

Internal Context [ISO Guide 73:2009, definition 3.3.1.2]	internal environment in which the organization seeks to achieve its objectives NOTE Internal context can include: - governance, organizational structure, roles and accountabilities; - policies, objectives, and the strategies that are in place to achieve them; - the capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies); - information systems, information flows and decision-making processes (both formal and informal); - relationships with, and perceptions and values of, internal stakeholders; - the organization's culture; - standards, guidelines and models adopted by the organization; and - form and extent of contractual relationships.
Issue	point of debate, discussion or dispute that requires resolution. An issue may be resolved as an uncertainty and therefore as a **risk** or as a certainty in which case it is a **problem**.
Level of Risk [ISO Guide 73:2009, definition 3.6.1.8]	magnitude of a **risk** or combination of risks, expressed in terms of the combination of **consequences** and their **likelihood**
Likelihood [ISO Guide 73:2009, definition 3.6.1.1]	chance of something happening NOTE 1 – In risk management terminology, the word "likelihood" is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period). NOTE 2 – The English term "likelihood" does not have a direct equivalent in some languages; instead, the equivalent of the term "probability" is often used. However, in English, "probability" is often narrowly interpreted as a mathematical term. Therefore, in risk management terminology, "likelihood" is used with the intent that it should have the same broad interpretation as the term "probability" has in many languages other than English.
Milestone [Wideman]	point in time representing a key or important intermediate **event** in the life of a **project**. A milestone should be capable of validation by meeting all of the items prescribed in a defining checklist as agreed with the **stakeholders**.
Monitoring [ISO Guide 73:2009, definition 3.8.2.1]	continual checking, supervising, critically observing or determining the status in order to identify change from the performance level required or expected NOTE - Monitoring can be applied to a **risk management framework**, **risk management process**, **risk** or **control**.
Optimism Bias [MOD, Risk Lexicon]	independent 'top down' assessment of risk, which recognises the demonstrated, systematic, tendency for appraisers to be over-optimistic about key project parameters.
Problem	an **event** that is certain to occur or a **risk** that eventuates, it must be managed through the project planning, **control**, decision making and other **processes**.
Process [AS/NZS 9000:2006]	set of interrelated or interacting activities that transforms inputs into outputs.
Project [adapted from AS/NZS 9000:2006 the PMBOK Guide 2008]	a temporary endeavour with defined start and finish dates undertaken to create a unique product or service in accordance with specified resources or requirements.
Project Charter [Wideman]	formal document providing authority to a project manager to conduct a project within scope, quality, time, cost and resource constraints as laid down in the document.
Project Metrics	system of measuring project parameters.
Residual Risk [ISO Guide 73:2009, definition 3.8.1.6]	**risk** remaining after **risk treatment** NOTE 1 - Residual risk can contain unidentified risk. NOTE 2 - Residual risk can also be known as "retained risk".
Resource [ISO/IEC 15288:2003]	an asset that is utilised or consumed during the execution of a process. Note 1 – Resources may include diverse entities such as personnel, facilities, capital equipment, tools and utilities such as power, water, fuel and communication infrastructures.

Responsibility [Wideman]	duties, assignments, and accountability for results associated with a designated position in the organization.
Review [ISO Guide 73:2009, definition 3.8.2.2]	activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives NOTE - Review can be applied to a **risk management framework**, **risk management process**, **risk** or **control**.
Risk [ISO Guide 73:2009, definition 1.1]	effect of uncertainty on objectives NOTE 1 - An effect is a deviation from the expected — positive and/or negative. NOTE 2 - Objectives can have different aspects (such as financial, health and safety, and environmental goals) and can apply at different levels (such as strategic, organization-wide, project, product and process). NOTE 3 - Risk is often characterized by reference to potential **events** and **consequences**, or a combination of these. NOTE 4 - Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** of occurrence. NOTE 5 - Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of, an event, its consequence, or likelihood.
Risk Analysis [ISO Guide 73:2009, definition 3.6.1]	process to comprehend the nature of **risk** and to determine the **level of risk** NOTE 1 - Risk analysis provides the basis for **risk evaluation** and decisions about **risk treatment**. NOTE 2 – Risk analysis includes risk estimation.
Risk Assessment [ISO Guide 73:2009, definition 3.4.1]	overall process of **risk identification**, **risk analysis** and **risk evaluation**
Risk Attitude [ISO Guide 73:2009, definition 3.7.1.1]	organization's approach to assess and eventually pursue, retain, take or turn away from **risk**
Risk Criteria [ISO Guide 73:2009, definition 3.3.1.3]	terms of reference against which the significance of a **risk** is evaluated NOTE 1 - Risk criteria are based on organizational objectives, and **external** and **internal context**. NOTE 2 - Risk criteria can be derived from standards, laws, policies and other requirements.
Risk Evaluation [ISO Guide 73:2009, definition 3.7.1]	process of comparing the results of **risk analysis** with **risk criteria** to determine whether the **risk** and/or its magnitude is acceptable or tolerable NOTE - Risk evaluation assists in the decision about **risk treatment**.
Risk Identification [ISO Guide 73:2009, definition 3.5.1]	process of finding, recognizing and describing **risks** NOTE 1 - Risk identification involves the identification of **risk sources**, **events**, their causes and their potential **consequences**. NOTE 2 - Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and **stakeholder**'s needs.
Risk Management [ISO Guide 73:2009, definition 2.1]	coordinated activities to direct and control an organization with regard to **risk**
Risk Management Framework [ISO Guide 73:2009, definition 2.1.1]	set of components that provide the foundations and organizational arrangements for designing, implementing, **monitoring**, reviewing and continually improving **risk management** throughout the organization NOTE 1 - The foundations include the policy, objectives, mandate and commitment to manage **risk**. NOTE 2 - The organizational arrangements include plans, relationships, accountabilities, resources, processes and activities. NOTE 3 - The risk management framework is embedded within the organization's overall strategic and operational policies and practices.

Risk Management Plan [ISO Guide 73:2009, definition 2.1.3]	scheme within the **risk management framework** specifying the approach, the management components and resources to be applied to the management of **risk** NOTE 1 - Management components typically include procedures, practices, assignment of responsibilities, sequence and timing of activities. NOTE 2 - The risk management plan can be applied to a particular product, process and project, and part or whole of the organization.
Risk Management Policy [ISO Guide 73:2009, definition 2.1.2]	statement of the overall intentions and direction of an organization related to **risk management**
Risk Management Process [ISO Guide 73:2009, definition 3.1]	systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, and identifying, analyzing, evaluating, treating, **monitoring** and reviewing **risk**
Risk Manager	responsible for operating the project's **risk management process** and the custodian of the **risk management plan** and **risk register**.
Risk Owner [ISO Guide 73:2009, definition 3.5.1.5]	person or entity with the accountability and authority to manage a **risk**
Risk Profile [ISO Guide 73:2009, definition 3.8.2.5]	description of any set of **risks** NOTE - The set of risks can contain those that relate to the whole organization, part of the organization, or as otherwise defined.
Risk Register	record, under formal change control, of all identified **risks**, their **risk assessment**, **risk treatment**s and outcomes.
Risk Source [ISO Guide 73:2009, definition 3.5.1.2]	element which alone or in combination has the intrinsic potential to give rise to **risk** NOTE - A risk source can be tangible or intangible.
Risk Treatment [ISO Guide 73:2009, definition 3.8.1]	process to modify **risk** NOTE 1 - Risk treatment can involve: - avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; - taking or increasing risk in order to pursue an opportunity; - removing the **risk source**; - changing the **likelihood**; - changing the **consequences**; - sharing the risk with another party or parties (including contracts and risk financing); and - retaining the risk by informed decision. NOTE 2 - Risk treatments that deal with negative consequences are sometimes referred to as "risk mitigation", "risk elimination", "risk prevention" and "risk reduction". NOTE 3 - Risk treatment can create new risks or modify existing risks.
Stakeholder [ISO Guide 73:2009, definition 3.2.1.1]	person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity NOTE - A decision maker can be a stakeholder.

ISO definitions reproduced with permission from SAI Global under Licence 1012-c110 available for purchase at http://www.saiglobal.com

Appendix 6 - References

Standards Australia/Standards New Zealand, *AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines*, Sydney: Standards Australia/ Standards New Zealand, 2009

New South Wales Treasury (2009), *TPP 09-05: Internal Audit and Risk Management Policy* available at http://www.treasury.nsw.gov.au/Internal_Audit_and_Risk_Management

Standards Australia/Standards New Zealand, *HB 327:2010 Communicating and Consulting about Risk,* Sydney: Standards Australia Limited, 2009

International Electrotechnical Commission, IEC/ISO 31010:2009 Risk Management – Risk Assessment Techniques, Geneva: IEC, 2009

International Organization for Standardization, *ISO Guide 73: 2009 Risk Management – Vocabulary*, Geneva: ISO, 2009

Standards Australia/Standards New Zealand, *HB 436:2004 Risk Management Guidelines Companion to AS/NZS 4360:2004*, Sydney: Standards Australia International Limited and Standards New Zealand, 2005

ISO/IEC 15288:2008 Systems engineering – System life cycle processes, USA: ISO/IEC-IEEE, 2008

DeMarco T & Lister T (2003); Waltzing with Bears – Managing Risk on Software Projects, New York: Dorset House, 2003

Software Engineering Institute, A Proposed Taxonomy for Software Development Risks for High-Performance Computing (HPC) Scientific/Engineering Applications, CMU/SEI-2006-TN-039, Carnegie Mellon University, 2007 located at http://www.sei.cmu.edu/reports/06tn039.pdf

Project Management Institute (2008), *PMBOK Guide – 4th Edition*, Pennsylvania: PMI, 2008

UK Ministry of Defence, *Risk Lexicon* available at http://www.aof.mod.uk/aofcontent/tactical/risk/downloads/risk_lexicon_v1.pdf

Wideman, M (2002), *Wideman Comparative Glossary of Common Project Management Terms v3.1* available at http://www.maxwideman.com/pmglossary/index.htm

NSW Department of **Finance and Services**

ICT Policy Branch
McKell Building
2-24 Rawson Place
Sydney NSW 2000
T: 02 9372 8877
F: 02 9372 8640
TTY: 1300 301 181
www.services.nsw.gov.au