

6 Risk Management

There are always risks associated with a project. The purpose of risk management is to ensure levels of risk and uncertainty are properly managed, so that the project is completed successfully. It enables those participants involved in a project to identify possible risks, the manner in which the risks can be contained and the likely cost of mitigation strategies.

Ultimate responsibility for ensuring appropriate Risk Management processes are applied rests with the Project Sponsor and Project Steering Committee. Processes for escalating business risks to Senior Management should occur as part of the overall Agency or whole-of-government risk management processes, including information and physical security risk management plans. Project Risk Management activities also should be conducted using Agency Risk Management processes where they exist.

The processes by which risks will be managed during the project should be documented in the Project Risk Management Plan, which can be included in the Project Business Plan or developed as a separate document, depending on the size and complexity of the project.

This section of the *Tasmanian Government Project Management Guidelines* includes:

- Risk Management - including a definition of risk
- Main elements of Risk Management
- Roles and responsibilities - in ensuring successful Risk Management
- Documentation - what a Risk Management Plan and Risk Register should cover

Definition

Risk refers to any factor (or threat) that may affect adversely the successful completion of the project in terms of delivery of its outputs or adverse effects on resourcing, time, cost and quality. These factors/threats include risks to the project's business environment that may prevent the project's outcomes/benefits from being realised fully.

Successful projects try to resolve risks before they occur - the art of Risk Management!

It should be noted that sometimes risks may be associated with opportunities, such as the use of a new technology, and acceptance of the risk needs to be based on the costs of rectifying the potential consequences versus the opportunities afforded by taking the risk.

Risk Management describes the processes concerned with identifying, analysing and responding to project risk. It consists of risk identification, risk analysis, risk evaluation and risk treatment. The processes are iterative throughout the life of the project and should be built into the project management planning and activities.

The Project Sponsor/Steering Committee has ultimate responsibility for oversight of the *Risk Management Plan*, including ensuring mitigation strategies are implemented, and identification of when mitigation actions will be undertaken, for all high-grade risks. All information should be documented in the *Risk Management Plan*.

Risk management is conducted initially as part of the assessment of the project's viability and documented in the *Project Proposal* or *Business Case*, depending on the

size of the project. This documentation occurs during the INITIATION Phase of the project. An ongoing review of risks should be conducted throughout the life of the project to ensure that changing circumstances are tracked and managed.

All projects require a degree of risk management, but the effort expended will depend on the complexity, size and scope, including outcomes/benefits, customers, outputs, work and resources. Large and/or complex projects, involving significant investment and/or major outcomes/benefits, require formal and detailed risk management activities on an ongoing basis.

Issues Management and Risk Management are closely linked, as some issues, if not managed, may become risks. This linkage is the reason why it is recommended that major issues also are identified and managed.

(Refer to Section 7: Issues Management)

6.1 Main Elements of Risk Management

The main elements of the Risk Management Process, as described in the *Australian Standard for Risk Management (AS/NZS4360: 2004)*, are shown below:

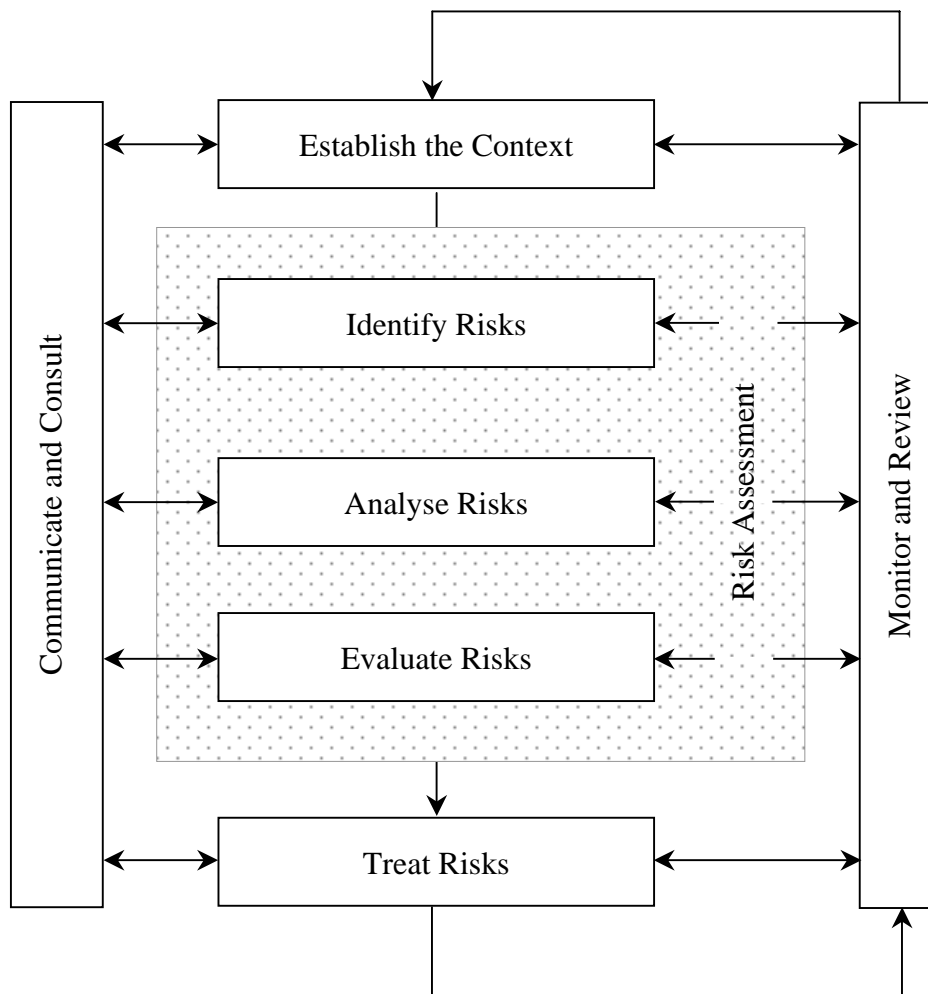


Figure 7: Elements of the Risk Management process

Communicate and Consult

Since stakeholders can have a significant impact on decisions made, it is important that their perceptions of risk be identified and documented, with the underlying reasons for the perceptions understood and documented. Communication and consultation with all Key Stakeholders should be an ongoing process and not just part of the initial risk identification and analysis process. This process can be tied in with the overall *Communication Strategy* for the project and need not be a separate activity.

Before developing the *Risk Management Plan* for large and/or complex projects, the Steering Committee and other Key Stakeholders should be brought together to undertake initial risk identification and analysis activities. As a minimum, changes in risk status must be reported to the Project Sponsor and the Steering Committee as part of the *Project Status Report*.

(Refer to the *Project Management Fact Sheet: Developing a Project Communication Strategy Plan* and the *Project Management Proforma: Project Status Report*)

Establishing the Context

The context for the risk management process is the business environment in which the project is being implemented. This context includes political, organisational and strategic sources of risk. The project scope, including outcomes/benefits, customers, outputs, work and resources, also forms part of the context and can help highlight potential sources of risk.

Identification of the context for the risk management processes must include, particularly in the case of large and/or complex projects, identification of risks to the business environment where the project operates. Processes for escalating business risks to Senior Management should occur as part of the overall Agency or whole-of-government risk management activities, including information and physical security risk management.

The Tasmanian Government Information Security Framework - Risk Management Guidelines recommend the adoption of a consistent risk management framework for all risk management activities within an Agency/organisation, which includes a single approach to determining and grading of likelihood, seriousness/impact and risk levels for all risk assessments conducted by the Agency/organisation.

The processes by which risks will be managed during the project should be documented in the *Project Risk Management Plan*, which can be included in the *Project Business Plan*, or developed as a separate document, depending on the size and/or complexity of the project.

Risk Identification

Before risks can be properly managed, they must be identified. A very broad identification, analysis and evaluation of project risks should form part of the *Project Proposal* and/or *Business Case*. Once the project has received approval to proceed, risk identification usually is done initially by involving Key Stakeholders, including Steering Committee members. Brainstorming sessions to identify and clarify the main risks, which may prevent the project achieving its stated outcomes/benefits, are one way of doing the identification.

It is important to define clearly the scope of the project at this stage so that the identification of risks can remain focused on what potentially threatens the delivery of outputs (level of resourcing, time, cost and quality) and the realisation of outcomes/benefits by the Business Owner(s). Risks also can be categorised, for

example in terms of type (ie Corporate Risks, Business Risks, Project Risks and System Risks). These categories can be broken down into other categories, including Diseases, Economic, Environmental, Financial, Human, Information and Physical Security, Natural Hazards, Occupational Health and Safety, Public Liability etc. Establishing categories can assist in ensuring all relevant risks are identified.

(Refer to the *Project Management Fact Sheet: Developing a Risk Management Plan*)

Another way of establishing categories is to take each of the Key Elements of project management, as outlined in *Section 1* of these Guidelines, and identify which risks may impinge on the application of each Key Element.

Once all risks have been identified, a filtering process should be used to determine which identified risks:

- Are best left, as the likelihood and seriousness would be so low that mitigation strategies are not required
- Need monitoring, but no proactive mitigation strategies required at this stage
- Are avoided by changing the scope of the work of the project, with appropriate sign-off
- Have to be escalated for the attention of Senior Management within the Agency as a risk to the overall Agency or whole-of-government business
- Need planned mitigation strategies, as detailed in the *Risk Register*

The results of this exercise should be documented in a *Risk Register* for the project.

Risk Analysis

Risks can be analysed according to the likelihood they will be realised and the level of seriousness/impact they will have if they do occur. That is, risks are classified whether there is a low, medium or high likelihood they will occur, and according to whether their level of seriousness/impact will be low, medium or high if they happen. From this classification, a priority listing for evaluation and action can be developed, separating the acceptable risks from the unacceptable ones.

Examples of possible risks might include a loss of funding (the effect of which is a lack of resources), an influenza epidemic (the effect of which crucial Project Team members become sick) or that crucial stakeholders are not interested in the project (the effect of which is they do not provide important input into the project or take responsibility for it).

Table 7 illustrates, at a simple level, how this analysis can be done using the examples above. Assessing the likelihood and seriousness of risks to a project provides a good indication of the project risk exposure.

Risk	Likelihood			Seriousness		
	Low	Med	High	Low	Med	High
Loss of funding		X		X		
Influenza epidemic			X			X
Lack of stakeholder commitment			X			X

Table 7: Example of risk analysis

In practice, it is often difficult to analyse the likelihood/seriousness of risks quantifiably and that is why a qualitative word scale often is used.

Risks analysed in *Table 7* can be graded easily using the risk matrix in *Table 8a*.

	Seriousness			
		Low (Insignificant adverse impact, note only)	Medium (Reasonable adverse impact, needs monitoring)	High (Will have significant adverse impact)
Likelihood	Low (Unlikely to occur during project)	E	D	C
	Medium (May occur at some stage in project)	D	C	B
	High (Probably will occur during project)	C	B	A

Table 8a: Risk matrix for grading risks

For example: Low Likelihood/Low Seriousness equates to an **E** grading for overall risk exposure. High Likelihood/Medium Seriousness equates to a **B** grading for the risk exposure.

In the case of large and/or complex projects, the matrix should be expanded to ensure an **A** Grading is automatically assigned to any risks defined as extremely high seriousness; that is, any risk which, if realised, will cause the project to fail. An example of an Extreme Risk to the project might be unexpected legislative changes.

	Seriousness				
		Low	Medium	High	EXTREME (Major adverse impact on project or Business Owner operations)
Likelihood	Low	E	D	C	A
	Medium	D	C	B	A
	High	C	B	A	A

Table 8b: Risk matrix for grading risks

The resulting **Grades** of risk help the Steering Committee and Project Team to focus on treating the most important risks, once analysed, evaluated and prioritised, and to mitigate them before the project progresses much further into the MANAGE Phase.

That is not to say that risks may not re-emerge after treatment and is why it is stressed that risk management is an iterative process throughout the life of the project.

Table 9 recommends the type of actions that should be used, and agreed to, in relation to each grade of risk.

Grade	Risk Mitigation Actions	Who
A	Mitigation actions, to reduce the likelihood and seriousness, to be identified, costed and prioritised for implementation before the project commences or immediately as they arise during project execution	Steering Committee/ Project Sponsor
B	Mitigation actions, to reduce the likelihood and seriousness, to be identified, costed and prioritised. Appropriate actions implemented during project execution	Steering Committee/ Project Manager
C	Mitigation actions, to reduce the likelihood and seriousness, to be identified and costed for possible action if funds permit	Project Manager
D & E	To be noted; no action is needed unless grading increases over time	Project Manager

Table 9: Recommended actions for grades of risk

There are more sophisticated tools available to assist with risk analysis and many include extensive numeric scales and algorithms. For very large and/or more complex projects, it is wise to investigate the use of these tools, although the approach above is a starting point and is easily explained to non-specialists. Levels in the *Risk Matrix* tables, for example, can be expanded to four or five depending on the nature and size of the project. **The approach above is just a suggested starting point.**

Risk Evaluation

Risk analysis helps those people involved with a project to evaluate and prioritise the most significant risks for careful management. Risk evaluation involves assessing the risks in order to prioritise those risks that should be addressed by treatment or mitigation plans. Once risks have been analysed and graded in terms of likelihood and seriousness they have to be evaluated. Risk evaluation involves monitoring and understanding the factors that can reduce project success and determining what is an acceptable or unacceptable risk based on agreed criteria.

Risks can result in four types of consequences:

- Benefits are delayed or reduced
- Timeframes are extended
- Costs are advanced or increased
- Output quality (fitness-for-purpose) is reduced

Once this evaluation has been undertaken decisions then can be made. For example, that a risk is acceptable in terms of extended timeframes, as the project is not tied strictly to set deadlines, but is not acceptable if it reduces the planned benefits or affects output quality. If, on the other hand, a project has fixed deadlines, then the decision might be made that the level of risk is acceptable in terms of reducing the quality of the outputs, with a view to enhancing quality after the initial deadline has been achieved.

Once priorities are agreed, mitigation strategies must be developed and implemented for all unacceptable risks.

Risk Mitigation/Treatment

Risk mitigation actions or treatment reduce the chance that a risk will be realised and/or reduce the seriousness of a risk that is realised. The costs of these actions should be identified as part of the EVALUATION activities. There are two broad types of risk mitigation or treatment activities:

- Preventative - planned actions to reduce the LIKELIHOOD a risk will occur and the SERIOUSNESS if it does occur. In other words, what can be done now? For example, if a risk were identified that the project's major clients will not have the technical expertise to utilise adequately the technology the project is implementing, an appropriate preventative action would be to provide technical training. Preventative actions for Grades A and B risks should be implemented before the project progresses very far into the MANAGE Phase.
- Contingency - planned actions to reduce the SERIOUSNESS of the risk if it does occur. In other words, what should be done if? For example, a possible action in response to the previous risk might be that ongoing technical support and advice is provided to the client Agency/organisation once the technology is implemented.

Risk mitigation or treatment actions should be cost efficient and effective in that they help reduce the risk exposure of the project. Conscious decisions need to be made regarding the wearing or transferring of certain risks as opposed to the costs of mitigation.

For serious risks, an extremely effective risk mitigation strategy can be justified more easily in terms of its cost. A portfolio of cost-effective risk mitigation actions forms part of the *Risk Register* for large and/or complex projects. Mitigation strategies to reduce the likelihood and seriousness of risks should be built into the budget and activities of the project. Mitigation strategies should be measured, comparing cost and benefits.

RECOVERY actions are those subsequent actions that allow you to move on after a risk has occurred. They include management of residual risks. Hopefully, the seriousness of a risk's impact on the project will have been reduced due to the planned contingencies being implemented. These recovery actions should be built into the work breakdown structure for the project. In other words - what should be done and when. A good example is disaster recovery planning in the case of a new IT system or, in the case of the previous example, the client organisation hired people with technical expertise as the ongoing IT support did not provide a final solution.

Monitor and Review

Risk management is not a one-off activity. Risks should be monitored throughout the project, as their likelihood or impact ratings may change or new risks and previously treated risks may emerge. As a guide, risks and the effectiveness of the mitigation strategies should be assessed approximately every two weeks. Over a long, significant project there should also be regular formal monthly reviews. It is important to remember that the whole process is iterative throughout the life of the project. Regular reporting, at agreed intervals, of **Risk Status** must be conducted by the Project Manager and must be required by the Project Sponsor/Steering Committee.

(Refer to the *Project Management Proforma: Project Status Report*)

6.2 Roles and Responsibilities

The **Project Sponsor** has ultimate accountability for risk management. They ensure there are adequate resources for managing the project's risks and there is adequate active participation in the risk management process by a wide cross-section of stakeholders. They ensure also that any corporate or Agency/organisation risks, identified during the project, are escalated for the attention of those people responsible for their management. They also monitor the progress and effectiveness of the *Risk Management Plan*.

The **Steering Committee** oversees the *Risk Management Plan* and its periodic review. It is accountable for ensuring an effective *Risk Management Plan* is in place throughout the life of the project, and that appropriate mitigation strategies are being implemented for all high-level risks.

The **Project Manager** is responsible for monitoring and managing all aspects of the risk management process under the direction of the Project Sponsor/Steering Committee, including:

- Developing the *Risk Register* and *Risk Management Plan*
- Continual monitoring of the project to identify any new or changed risks
- Implementing the planned mitigation strategies
- Continual monitoring of the effectiveness of the *Risk Management Plan*
- Regular reporting on the status of risks to the Project Sponsor and the Steering Committee

In large projects, the Project Manager may choose to assign risk management activities to a separate Risk Manager, but the Project Manager should still retain responsibility. It should be noted that large projects are a risk, and the need for the Project Manager to reassign this integral aspect of project management may be an indication that the project should be re-scoped or divided into several sub-projects, overseen by a Project Director.

It is important also to remember that the person directly responsible for risk management does not generally conduct all risk management assessments themselves, but facilitates the analysis by involving relevant people, particularly Key Stakeholders, and by providing appropriate mechanisms for discussion and documentation.

Other **Project Team members** are some of the people who can assist with the identification, analysis and evaluation of risks, and can assist in the development of the *Risk Management Plan*. They can also be responsible for risk mitigation actions.

Project Stakeholders, Steering Committee, Reference Groups, external consultants, and importantly, the Business Owner(s) should provide input into the *Risk Management Plan*, especially assessment of potential risks and risk mitigation actions. They may also be allocated responsibility for some risk mitigation actions.

It is important to remember risk management cannot be the responsibility of one person entirely, and that it is a communal activity involving a range of people associated with the project.

(Refer to the *Project Management Fact Sheet: Developing a Risk Management Plan*)

6.3 Documentation

Risk Management Plan

A *Risk Management Plan* should be included as a section in the *Project Business Plan*, or as a separate document, depending on the size of the project, and should cover, at a minimum, the following:

- The process for identification, analysis, evaluation and treatment of risks, both initially and throughout the life of the project, including estimated costings
- The process for transferring approved risk costings into the project budget
- The process for transferring risk mitigation activities into the project Work Breakdown Structure
- How often the *Risk Register* will be reviewed, the process for review and who will be involved
- How Risk Status will be reported and to whom
- Who will be responsible for which aspects of risk management
- Include, as an appendix, a snapshot of the major risks, current gradings, planned mitigation strategies and costings, and who will be responsible for implementing any mitigation strategies (the snapshot may be a copy of the *Risk Register*)

Risk Register

A *Risk Register* is a useful tool for outlining all the risks identified before and during the project, for keeping a record of their grading in terms of likelihood and seriousness and a record of the proposed mitigation strategies, costings and responsibilities. The *Risk Register* forms the basis for the *Risk Management Plan*. In small projects, the *Risk Register* is the *Risk Management Plan*. In large and/or more complex projects, a more detailed *Risk Management Plan* should be developed for approval by the Steering Committee.

The *Risk Register* should cover:

- A unique identifier for each risk
- A description of each risk, and how it will affect the project
- An assessment of the likelihood it will occur, and the possible seriousness if it does occur (low, medium, high)
- A grading of each risk according to a risk assessment table (eg *Table 8a* or *8b*)
- A description of the mitigation strategies, which can include preventative (to reduce the likelihood) and contingency actions (to reduce the seriousness)
- Who is allocated responsibility
- In large and/or more complex projects, costings of each mitigation strategy

(Refer to the *Project Management Proforma: Risk Register*)