

Frequently Asked Questions: Risk Management

Version 1.2 – October 2007

DISCLAIMER

This material has been prepared for use by Tasmanian Government agencies and Instrumentalities. It follows that this material should not be relied upon by any other person. Furthermore, to the extent that 'this material is relied upon', the Crown in Right of the State of Tasmania gives no warranty as to the accuracy or correctness of the material or for any advice given or for omissions from the material. Users rely on the material at their own risk.

What are the benefits of risk management?

The benefit of risk management is to increase the likelihood that the project will be completed successfully by ensuring levels of risk and uncertainty in the project is properly managed. It enables those involved to identify possible risks, the manner in which they can be contained and the likely cost of mitigation strategies.

What is a risk?

A risk is any factor (or threat) that may adversely affect the successful completion of the project in terms of achievement of its outcomes, delivery of its outputs or adverse effects upon resourcing, time, cost and quality.

How do I identify risks?

Risk identification is often done by using brainstorming sessions to identify and clarify the main risks that may work against the project achieving its stated outcomes, output delivery or adverse effects upon resourcing, time, cost and quality. It is important to clearly define the scope of the project so that the identification of risks can remain focused upon what potentially threatens the achievement of outcomes, delivery of outputs, level of resourcing, time, cost and quality.

Establishing categories can also assist in making sure all relevant risks are identified. For example categories might include Corporate Risks, Business Risks, Project Risks and System Risks or categories such as environmental, economic, human, etc. Other ways to categorise risks are in terms of risks external to the project and those that are internal, or to take each of the key elements of project management as outlined in Section 1 of the Tasmanian Government's *Project Management Guidelines* and identify which risks may

impinge upon the successful application of each of these.

For large/complex projects the *Risk Identification Tool* may provide some useful prompts to assist in risk identification.

Does my project have risks?

There are always risks associated with a project. Therefore all projects require a degree of risk management, but the effort expended will depend on the size and scope of the project, including outcomes, customers, outputs, work and resources. Larger/complex projects involving significant investment and/or major outcomes require formal and detailed risk management activities to be undertaken on an ongoing basis.

Can a risk be a 'nonsense/irrelevant' risk?

Once all risks have been identified, those risks where the likelihood and seriousness are negligible and thus do not require mitigation strategies may be ignored (for example, a major natural disaster such as a severe earthquake in Tasmania).

When is a risk no longer a risk?

A risk is no longer a risk when it no longer is a factor (or threat) that may adversely affect the successful completion of the project. This is usually as a result of mitigation strategies taken, if the threat has been realised, or if there has been a change in the environment that makes the risk no longer relevant.

Is it still worthwhile to do risk management when a project is half over?

Yes, there are still risks associated with a project even if it is half over. This also forms a baseline for the remainder of the project.

What is the difference between a risk and an issue?

An issue is a problem or concern that may impede the progress of the project if not addressed.

A risk is any factor (or threat) that may adversely affect the successful completion of the project in terms of achievement of its outcomes, delivery of its outputs or adverse effects upon resourcing, time, cost and quality.

What is the relationship between the Issues Register and the Risk Register?

The *Issues Register* contains problems/concerns that may impede the progress of the project. The *Risk Register* contains the threats to the successful completion of the project.

An issue may be elevated from the *Issues Register* to the *Risk Register* if the issue cannot be resolved and becomes a threat to the project's success. In some cases a threat may cease to be a threat but remain an issue in which case it would be transferred from the *Risk Register* to the *Issues Register*.

On what basis should I elevate an Issue to a Risk?

If the issue cannot be resolved and becomes a threat to the successful completion of the project, then it becomes a risk and should be added to the *Risk Register*.

Who is responsible for risk management?

Many people involved in a project have some responsibility for project risk management including the Project Manager, Steering Committee, Project Sponsor, potential Business Owners, project Team Members and working groups. It is important that they know that

watching out for and reporting potential risks is a significant part of their role.

The **Project Sponsor** has ultimate accountability for Risk Management. This includes ensuring that there are adequate resources for managing the project's risks and that there is adequate active participation in the risk management process by a wide cross-section of stakeholders. The Project Sponsor also monitors the progress and effectiveness of the *Risk Management Plan*.

The **Steering Committee** oversees the *Risk Management Plan* and is responsible for its periodic review to ensure it adequately reflects an appropriate risk management approach for the project. They are responsible for ensuring an effective *Risk Management Plan* is in place throughout the life of the project. The Steering Committee is also responsible for regularly reviewing the *Risk Register* to ensure all high-level risks are being appropriately managed. Their role would include such things as:

- approving mitigation actions
- identifying new/alternative actions
- identifying new risks.

Members of the Steering Committee may also be responsible for undertaking some risk mitigation actions.

The **Project Manager** is responsible for monitoring and managing all aspects of the risk management process including:

- the development of the *Risk Register* and *Risk Management Plan*
- the continual monitoring of the project to identify any new or changed risks, and updating the Risk Register accordingly
- continual monitoring of the effectiveness of the Risk Management Plan
- regular reports on the status of risks to the Project Sponsor and Steering Committee.

Project Stakeholders, reference groups, external consultants and especially the Business Owners should provide input into the *Risk Management Plan* and especially assessment of potential risks and risk mitigation actions.

Who should identify risks?

For a medium to large project, the risks are identified by, (as a minimum), the Project Manager, Project Team members, Steering Committee members, Business Owners and external key stakeholders by the use of a number of meetings or brainstorming sessions.

For a small project, the Project Manager may identify risks and develop the *Risk Register*, perhaps with input from the Project Sponsor/Senior Manager and colleagues or a small group of key stakeholders.

For large/complex projects, it is often advisable to use an outside facilitator. Preparation may include an environmental scan, seeking views of key stakeholders etc. Reference to the *Risk Identification Tool* may also provide some useful prompts.

Who should be involved in risk reviews?

For a medium to large/complex project, the risks are reviewed by the Project Manager, Project Team members, Steering Committee members and external key stakeholders.

For a small project, the Project Manager may review risks and update the *Risk Register*, with input from the Project Sponsor/Senior Manager and colleagues, or key stakeholders.

Who is the responsible for monitoring risks?

The Project Manager is responsible for monitoring and managing all aspects of the risk management process. In

large/complex projects, the Project Manager may choose to assign risk management activities to a separate Risk Manager, but they should still retain responsibility. Risks should be monitored throughout the project as their likelihood or seriousness ratings may change and new risks may emerge.

Who approves risk mitigation actions and/or their associated costs?

Each mitigation action needs to be costed as part of the risk evaluation process. On the basis of the risk grading and the associated mitigation costs, a decision will be made as to whether to undertake the mitigation action. The Project Manager may make this decision, if it is within their level of responsibility and the cost within their budget, otherwise Steering Committee or Sponsor approval may be required.

How do I (the Project Manager) report progress on risks?

Risk Status should be reported to the Steering Committee or Project Sponsor/Senior Manager on an agreed regular basis and form part of the Project Status reporting processes.

How do I describe the risk?

Phrasing of the risk should use a 'newspaper headline' style statement – short, sharp and snappy (eg. 'Inadequate funding to complete project').

What is a risk 'trigger'?

Consider what might be a 'trigger' event or threat (eg. 'poor quality materials causes costs to rise', 'project funding redirected', 'inaccurate supplier estimates cause cost increase' etc). Several triggers may reveal the same inherent risk (ie. 'Inadequate funding to complete project').

How do I describe the impact on the project?

Include a short statement that describes the nature of the risk and the impact on the project if the risk is not mitigated or managed (eg. 'Budget blow out means project delayed or abandoned, expenditure to date wasted, outcomes not realised, government embarrassed' or 'Budget blow out means cost savings must be identified – ie. reduce output quality, extended timeframes, outcomes (benefits) will be delayed.')

What is a preventative action?

A preventative action is a planned action to reduce the likelihood a risk will occur and the seriousness if it does occur. In other words, what should you do now? For example, if an identified risk is that the project's major clients will not have the technical expertise to adequately utilise the technology the project is implementing, an appropriate preventative action is to provide technical training.

What is a contingency action?

A contingency action is a planned action to reduce the seriousness of the risk, if it does occur. In other words, what should you do if the threat is realised? For example, if an identified risk is that the project's major clients will not have the technical expertise to adequately utilise

the technology the project is implementing, an appropriate contingency action might be the provision of ongoing technical support and advice to the client organisation once the technology is implemented.

What is a recovery action?

A recovery action is a subsequent action that allows you to move on after a threat has been realised. Hopefully, the seriousness of the risk's impact on the project will have been reduced due to the preventative actions and planned contingencies implemented. Once realised the recovery actions should be built into the *work breakdown structure* for the project. In other words, what should you do when? An example of this is disaster recovery planning in the case of a new IT system. Another example is when an identified risk is that the project's major clients will not have the technical expertise to adequately utilise the technology the project is implementing; an appropriate recovery action might be that the client organisation actually hires people with the technical expertise as the ongoing support has not provided a final solution.

When are these mitigation actions implemented?

The grade of the risk determines when the mitigation action is undertaken. The following table indicates when the action should be undertaken.

Grade	Risk Mitigation Actions
A	Mitigation actions to reduce the likelihood and seriousness to be identified and implemented as soon as the project commences.
B	Mitigation actions to reduce the likelihood and seriousness to be identified and appropriate actions implemented during project execution.
C	Mitigation actions to reduce the likelihood and seriousness to be identified and costed for possible action if funds permit.
D & N	To be noted; no action is needed unless grading increases over time.

What are the benefits of costing the actions?

As part of the process of developing the risk mitigation actions the costs associated with those actions need to be identified. The 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 acceptance of certain risks as opposed to the costs of mitigation.

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

plan of the project. Mitigation strategies will need to be measured comparing the cost versus effectiveness.

How are risks graded?

Risks can be evaluated 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 that they will occur, and according to whether their level of seriousness/impact will be low, medium or high if they happen.

The table below illustrates how this evaluation can be done. 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

The risks evaluated are then graded using the risk matrix in the following table. For the example, above this would result in a grade of D for the loss of funding and an A for each of the other two risks.

Likelihood	Seriousness			
		low	medium	high
low		N	D	C
medium		D	C	B
high		C	B	A

In the case of larger or more 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 or stop. An example is unexpected legislative changes.

Likelihood	Seriousness				
		low	medium	high	EXTREME
low		N	D	C	A
medium		D	C	B	A
high		C	B	A	A

Do I need to categorise risks?

No, categorisation of risks is only one way of identifying and managing risks. Larger projects will usually find this a useful tool in identifying and monitoring them.

How much risk management is needed for a small project?

The short answer is not much! The amount of risk management required is directly related to the complexity of the project; a large and/or complex project will have more risks than a small project.

For a small project, the *Risk Register* should be reviewed fortnightly for A and B grade risks with re-evaluation of all risks occurring on a monthly basis. This will entail the Project Manager doing a quick scan.

When should a risk be escalated?

If the likelihood or seriousness of a risk increases, then the grading of the risk will usually increase. The action to be taken will depend on the subsequent grading, for example if the risk goes from C to a B grading, then the action taken would change from just monitoring the risk to implementing the mitigation actions. This should be picked up during the risk monitoring process.

What is a 'killer' (extreme) risk?

Any risks defined as extremely high seriousness may be thought of as a 'killer' (extreme) risk. These are risks that, if realised, will cause the project to fail or stop. An example is unexpected legislative changes. An A Grading is automatically assigned to these risks, even if there is a low likelihood of the threat being realised.

What level of risk can stop a project?

This is dependant on the level of risk tolerance that is acceptable. In some cases there is a very low risk tolerance, for

example where lives are at risk, while in other cases the potential benefits may be such that there is a very high risk tolerance, for example in research and development projects.

How many risks should I have?

The number of risks tends to be proportional to the size and complexity of the project. Some projects have a high level of risk associated by their very nature. For example, so called 'bleeding edge' projects, which have a high degree of innovation and new ground is being broken, will have many risks.

How often should the risk register be reviewed?

The *Risk Register* should be reviewed fortnightly for A and B grade risks with re-evaluation of all risks occurring on a monthly basis. The size/complexity of the project will determine how thoroughly this is performed. A small project may only require a quick scan of the risks while a large/complex project requires a more detail examination of each risk. If your prevention strategies are effective, some of your Grade A and B risks should be able to be downgraded early in the project.

How much time should be spent on risk management?

This is directly related to the size, complexity and level of risk associated with the project. Larger projects require more time spent on risk management. As a guide, risks and the effectiveness of the mitigation strategies, should be assessed about every two weeks. Over a long, significant project, there should also be regular formal monthly reviews to confirm existing risks and identify new risks. The time taken for these depends on the size of the *Risk Register*. In some large projects, a Risk Management specialist may be employed due to the workload involved.

Where to get additional help

- Refer to the *Risk Register template* and *Risk Management Plan template*.
- Refer to the *Risk Identification Tool*.
- The *Tasmanian Government Project Management Guidelines*.
- The *Project Management Knowledge Base*.
- Contact Project Services on email pminfo@dpac.tas.gov.au.

Acknowledgements

Elements of this FAQ have been derived from the Australian Standard AS/NZS 4360:2004.

This FAQ also contains elements of the *Tasmanian Government Project Management Guidelines*, the *Project Business Plan template*, the *Risk Register template* and *Risk Management Plan template* prepared by the Department of Premier and Cabinet.