

Risk Management

Associated policy

Risk Management Policy

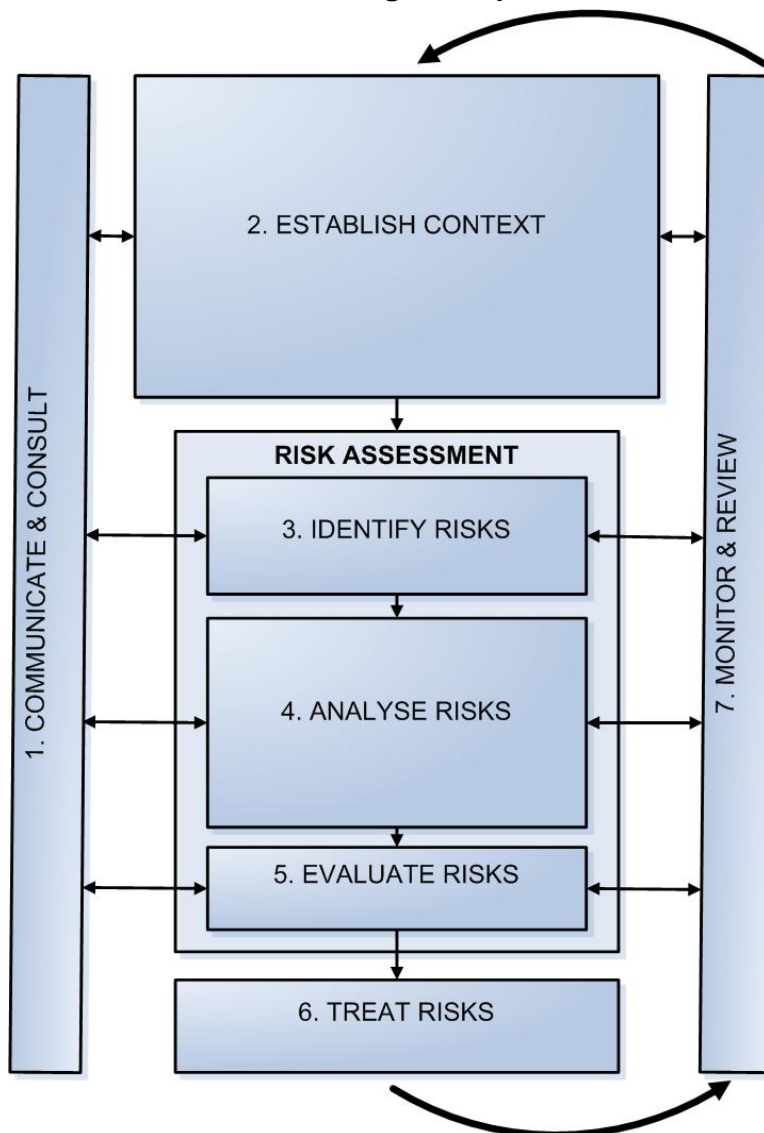
Definitions

See - [Attachment 1](#)

Actions

This procedure is based on the risk management process identified in *AS/NZS ISO 31000:2009 Risk management – Principles and guidelines*. The risk management process involves seven steps: communicate and consult; establish context; assess risks (identify risks, analyse risks and evaluate risks); treat risks; and monitor and review.

The risk management process



Step 1 - Communicate and consult: stakeholders' perspectives are considered at each stage to obtain or provide relevant risk information

- Consider stakeholder and client perspectives at each step of the risk management process.
- Consult widely using internal (organisational) and appropriate external (strategic) communication to ensure that those responsible for implementing risk management, and those with a vested interest, understand how decisions are made and why particular actions are required.
- Consult people who have appropriate knowledge of the risks to ensure that all relevant information is assessed.

Step 2 - Establish context: the environment and boundaries that should be applied when considering risks

- Consider factors that influence risks and their level – e.g. Queensland Water Commission (Commission) objectives, internal and external environments and key stakeholders. The risk context should be broadly defined to include a wide range of trends, influences and time horizons and enable the identification of emerging risks.
- Scan the external and internal business environment for trends, influences and anything else that may impact on the Commission's overall operating environment.
- Determine the specific risk context and organisational level within which risks will be managed (i.e. activity, project, business unit, business group, Commission, etc).
- Examine the objectives and intended outcomes of the business activity. Refer to the Commission's Strategic Plan, operational plans, project plans and any other relevant plans. Identify strategies, legislation and processes in place to achieve these objectives and outcomes.
- Identify critical factors in the internal and external business environment (e.g. political, organisational, social, economic, legal, technological, cultural and environmental). Identify the organisation's strengths, weaknesses, opportunities and threats.
- Identify internal and external stakeholders and how they could be affected by the consequences of risks. Develop an understanding of stakeholder perceptions of risks.

Step 3 - Identify risks: describing risks in terms of what can happen and the impact that can result

- Identify business objectives from relevant strategic, business and/or project plans that need to be assessed.
- Consider potential sources of risk as identified in [Step 2](#).
- Also consider factors in the internal and external environment that could impact on objectives such as stakeholder and client relationships, maintaining the Commission's reputation, legislative compliance, effective corporate governance, and effective management of the Commission's human, financial, physical, technological, information and other resources.
- Identify and describe the risk events that may arise in the business environment, the source of each risk and its area or areas of impact. Note that a risk could impact on more than one objective, e.g. inability to recruit suitable staff could limit the ability to deliver a range of services.

Step 4 – Analyse risks: rate each risk in terms of consequences and likelihood, to establish the risk level

- Identify any existing processes to control risks and assess their effectiveness (e.g. effective, partially effective or ineffective). As well as reducing risk levels, controls can sometimes create undue burdens or have weaknesses that need to be identified, so consider their impact and if necessary identify alternative approaches.
- Analyse each risk using the table in [Attachment 2](#) and taking into consideration existing controls to determine its consequences for the Commission.
- Examine all impact areas in the table but disregard those that are not relevant to your particular risk. Where more than one impact category is relevant, select the one with the highest consequences to arrive at one consequence level for the particular risk.
- Determine the likelihood of the risk occurring taking into consideration any existing controls using the Likelihood Table in [Attachment 2](#). Likelihood is a frequency measure indicating how often an event is likely to occur based on historical data and estimates. Use quantitative descriptions when there is operational or other data to support its use (e.g. long term accident, incident or near miss rates), otherwise use qualitative descriptions.
- Use the Risk Analysis Matrix in [Attachment 2](#) to determine the risk level for each risk. Combine the consequence and likelihood ratings by finding the intersection of the relevant consequences column and likelihood row to determine the risk level (i.e. Low, Medium, High or Extreme).

Step 5 - Evaluate risks: determine which risks require treatment or whether risks can be tolerated without treatment

- Prioritise risks for action by their assessed risk level and risk scale using the Risk Evaluation Table in [Attachment 3](#).
- Decide whether each risk requires treatment or whether approval should be sought from the appropriate General Manager to tolerate the risk.

Step 6 - Treat risks: identify options for treating intolerable risks and implement those most appropriate to reduce the risk level

- Identify risk treatment options for each risk in accordance with the assessed risk levels (see [Attachment 4](#)). Consider at least the following treatment options:
 1. tolerate (accept) the risk
 2. avoid the risk
 3. share the risk
 4. reduce or control the risk likelihood
 5. reduce or control the risk consequences
- Assess the identified treatment options, considering feasibility, costs and benefits, and select the most appropriate strategies.
- Document the treatment and seek approval from the responsible officer (risk owner – e.g. Director, General Manager).
- Record risk assessment, treatments, the position responsible for treating the risk and the associated timeframes in a risk register. A review date should be set to monitor treatment progress and/or re-assess the risk. Risk registers are maintained in TRIM (CF/10/1425).
- Implement the risk treatment.

Step 7 - Monitor and review: periodically report and review risks, their level, and progress on treatments

- Record and maintain full details of each risk in local risk registers, where appropriate. Risks that warrant concern and risks being treated must be documented in risk registers.
- Business Groups must monitor, review, analyse and update risk registers quarterly and must report risks as part of their regular (monthly and/or quarterly) reporting arrangements.
- Identify and report to the relevant Executive Management Team (EMT) member any strategic, high and extreme risks which cannot be managed locally.
- Corporate Strategy, Department of Environment and Resource Management will coordinate the reporting process and submit a consolidated report of risks to the EMT, including any for proposed inclusion in the Commission's Strategic Risk Register. The EMT will review and approve the Strategic Risk Register and ensure action is taken to mitigate the risks. Each EMT member will provide feedback to risk owners as required.
- The management of strategic risks will generally be dealt with by the Commission. It is only when the Commission considers the risk cannot be managed internally that it is required to be escalated into the whole-of-government risk management framework.
- Whole-of-government strategic risks may be considered at Strategic Cabinet meetings and through the State Budget process. Strategic risks that are identified at other times during the year that may affect whole-of-government can also be escalated through regular Cabinet meetings and Cabinet Budget Review Committee (CBRC) deliberations
- The General Manager, Strategic Governance and Risk will report periodically to the Audit and Risk Management Committee and EMT on risk management coordination in the Commission.
- Project managers must report significant project risks to their project board. Extreme or high project risks may need to be referred to when they are considered strategic risks. Project risks will be reviewed monthly as part of monthly progress reports.

Supporting documents

AS/NZS ISO 31000:2009 *Risk management—Principles and guidelines*
Draft Queensland Government Risk Management Guidelines 2011
Strategic and Operational Risk Registers

Procedure



Next review date

May 2012

Contact area or person

Policy owner: General Manager, Strategic Governance and Risk

Approval

Signed:

Gayle Leaver

A/Chief Executive Officer

Queensland Water Commission

Date:

Version history

Date	Action	Description/comments
16 May 2011	Version 2	Update to existing procedure
9 August 2011	Version 2.1	Update to incorporate Commissioner feedback
7 September 2011	Version 2.2	Update to reflect reporting processes
15 September	Version 2.3	Update to incorporate CEO Feedback
5 October 2011	Version 2.4	Update to Impact Table following Commission meeting feedback

Definitions

Action: An activity that can be undertaken and that has an assigned responsible person and a deadline. Actions can include setting up systems of controls.

Areas of impact: Risks may impact on any areas related to the organisation and its objectives. E.g. assets, revenue, costs, people, organisational performance, the community, the environment, organisational reputation, etc.

Consequence: The outcome or impact of any risk event. It may be expressed qualitatively or quantitatively and may be a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with each event.

Control: A process, policy, device, practice or other action that acts to modify or minimise risk.

Commission's workforce: All permanent, temporary and casual employees, contractors and volunteers.

Event: The occurrence of a particular set of circumstances

Identified risk: A risk identified in the risk management process and recorded in a risk register for further action.

Likelihood: The chance of something happening. It is a qualitative or quantitative description of the probability or frequency of an event occurring.

Operational risk: A risk that could impact on the effectiveness or efficiency of the Commission's operations.

PESTLE: political, economic, social, technological, legal and environmental.

Residual risk: The risk remaining after the implementation of risk treatments.

Risk: The chance of something happening that will have an impact on objectives. That is, the effect of uncertainty on objectives. It is measured by combining the consequences and likelihood of a risk event.

Risk analysis: A systematic process to understand the nature of and to determine the level of risk.

Risk assessment: The overall process of risk identification, risk analysis and risk evaluation.

Risk level: The level of risk calculated by combining likelihood and consequence, which expresses the significance of a risk to the organisation. It is the assessed level of the current risk with any existing controls in place.

Risk management: The comprehensive process of assessing and responding to risks. It includes managing adverse impacts and realising potential opportunities.

Risk management framework: The policy, procedures and systems developed and implemented by the Commission to manage risks.

Risk mitigation strategies: Planned approaches to reduce risk levels, as detailed in risk registers and risk treatments.

Risk owner: The person or position responsible for ensuring a specific risk is appropriately managed and reported.

Risk register: The collective record of identified risks, risk levels and action taken or to be taken to mitigate these risks.

Risk register owner: The manager responsible for maintaining a risk register.

Risk treatment: The selection and implementation of appropriate actions for dealing with risks.

Sources of risk: Factors contributing to potential risks or where risks are likely to originate. E.g. human behaviour, safety procedures, equipment failure, natural hazards, political circumstances, economic factors, technological change, policy change, etc.

Strategic risk: A risk that could affect the achievement of the Commission's vision and strategic objectives (as detailed in the Strategic Plan or Service Delivery Statement). These risks would usually be at high or extreme risk levels and may affect the whole Commission or more than Business Group.

SWOT: strengths, weaknesses, opportunities and threats.

Tolerable risk: The residual risk remaining after controls or treatments have been fully applied to risks that have been properly assessed and where the risk is as low as reasonably practicable (i.e. no additional treatment is feasible).

Queensland Water Commission Consequence and Impact Table

Impact Area	Consequence				
	Insignificant	Minor	Moderate	Major	Catastrophic
Business Delivery	Risk dealt with through routine operations	Minimal impact on delivery of strategic or business outcomes	Moderate impact on delivery of strategic or business outcomes	Impaired delivery of strategic or business outcomes	Strategic or business outcomes unable to be delivered
Financial	Small financial loss that can be absorbed by the Business Group.	Financial loss requiring reprioritisation and/or reallocation of available Business Groups funds	Financial loss requiring special allocation of Commission funds	Substantial financial loss requiring supplementary Treasury funding	Disastrous financial loss with severe Commission or State impact
	Financial loss or budget shortfall of < \$50k	Financial loss or budget shortfall of \$50k - \$100k	Financial loss or budget shortfall of \$100k - \$1m	Financial loss or budget shortfall of \$1m - \$5m	Financial loss or budget shortfall of > \$5m
Health and Safety	No injuries or only first aid treatment required	Minor injury or sickness requiring medical treatment	Serious injury or sickness requiring medical treatment	Single fatality or injuries requiring hospitalisation	Multiple fatalities
Human Resources	Insignificant staff turnover and/or absenteeism	Minor staff turnover and/or absenteeism	Moderate staff turnover and/or absenteeism	Major staff turnover and/or absenteeism	Chronic staff turnover and/or absenteeism
	Minimal vacancy rate	Minor issues filling vacancies	Difficulty filling vacancies within a Business Group	Inability to fill vacancies in multiple Business Groups	Inability to fill vacancies across the Commission
	Insignificant skill shortage	Skill shortage with minimal impact on work programs	Skill shortage impacting on delivery of services and/or projects	Substantial skill shortage significantly delaying key projects	Chronic skill shortage preventing the Commission undertaking its functions
Legal and Regulatory	Risk dealt with through routine operations	Minor legal issues	Legal issues and exposure to litigation	Major legal issues or litigation	Extreme legal issues or major litigation
		Censure by Regulators	Fines and/or penalties by Regulators	Restriction of business by Regulators	Cessation of business imposed by Regulators
Reputation	No adverse impact on Commission's reputation	Minor impact on the Commission's reputation	Adverse impact on the Commission's reputation	Major damage to the Commission's reputation	Irreparable damage to Commission's reputation
	No stakeholder and/or client sensitivity issues	Low stakeholder and/or client sensitivity	Moderate stakeholder and/or client sensitivity	Significant stakeholder and/or client sensitivity	Very high stakeholder and/or client sensitivity

LIKELIHOOD TABLE		
Likelihood	Qualitative description	Example of a quantitative description
Almost Certain	The event is expected to occur in most circumstances	May occur once a year or more frequently
Likely	The event will probably occur in many circumstances	May occur once every 3 years
Possible	Identified factors indicate the event could occur at some time	May occur once every 10 years
Unlikely	The event could occur at some time but is not expected	May occur every 30 years
Rare	The event may occur only in exceptional circumstances	May occur once every 100 years

RISK ANALYSIS TABLE					
CONSEQUENCES					
LIKELIHOOD	Insignificant	Minor	Moderate	Major	Catastrophic
Almost Certain	Medium (11)	Medium (16)	High (20)	Extreme (23)	Extreme (25)
Likely	Low (7)	Medium (12)	High (17)	High (21)	Extreme (24)
Possible	Low (4)	Medium (8)	Medium (13)	High (18)	Extreme (22)
Unlikely	Low (2)	Low (5)	Medium (9)	Medium (14)	High (19)
Rare	Low (1)	Low (3)	Low (6)	Medium (10)	Medium (15)

Risk evaluation table

Risk Level	Risk Scale	Action Required
EXTREME	22-25	<p>Immediate action and involvement required at Chief Executive Officer (CEO)/Commissioner level to control the risk</p> <p>The CEO/Commissioner may advise the Minister as appropriate</p> <p>Immediately report the risk to the CEO</p> <p>The CEO will approve appropriate treatment action where it is a strategic risk or where the responsible General Manager is unable to implement treatments to reduce an operational risk to a tolerable level</p> <p>The responsible General Manager (risk owner) for the risk is to actively manage the approved risk treatments</p> <p>Frequent monitoring and reporting to the Executive Management Team (EMT) of the progress of risk treatments is required</p>
HIGH	17-21	<p>Requires CEO/EMT attention and management responsibility to be specified to control the risk</p> <p>Report the risk to the CEO or relevant EMT member</p> <p>The CEO will approve appropriate EMT endorsed treatment action where it is a strategic risk or the responsible General Manager is unable to implement treatments to reduce an operational risk to a tolerable level</p> <p>The responsible General Manager (risk owner) for the risk is to actively manage the approved risk treatments</p> <p>Frequent monitoring and reporting of the progress of risk treatments is required</p>
MEDIUM	8-16	<p>Risk can be managed locally by specific monitoring or response procedures</p> <p>Management responsibility for the risk is to be specified</p> <p>Responsible General Manager (risk owner) is to approve and manage risk treatments or approve tolerating the risk without further treatment where appropriate</p> <p>Monitoring and reporting of the progress of risk treatments is required</p>
LOW	1-7	<p>Risk can be managed by routine procedures or established controls</p> <p>General Manager (risk owner) to oversee implementation of treatments or approve tolerating the risk without further treatment where appropriate</p> <p>Risk monitoring and reporting on an as needed basis</p>

Risk Treatment Options

Option	Description
Tolerate the risk	After controls have been applied there may be residual risks remaining that, after consideration and evaluation, are determined to be as low as practicably possible. A decision may therefore be made to tolerate or accept the risk (at its current risk level).
Avoid the risk	This may involve an informed decision not to proceed with or become involved in an activity, removing the aspect of the activity that is a source of risk or finding another way to achieve the same business outcome by changing the local circumstances, venue, equipment, etc.
Share the risk	This involves another party bearing or sharing some part of the risk. This may include the use of contracts, insurance policies and organisational arrangements such as partnerships and joint ventures.
Reduce or control the risk likelihood	<p>Treatment actions may include:</p> <ul style="list-style-type: none"> • audit and compliance programs which monitor or check treatment actions in place • contract conditions • formal reviews of requirements or operations • inspections and process controls • project management • preventative maintenance • quality assurance • research and development • structured training • supervision • testing • organisational arrangements • technical controls.
Reduce or control the risk consequences	<p>Treatment actions may include:</p> <ul style="list-style-type: none"> • contingency planning • business continuity management • contractual arrangements and contract conditions • design features • disaster recovery plans • fraud control planning • minimising exposure to sources of risk • engineering and structural barriers • pricing policy and controls • separation or relocation of an activity and resources • reduction of inventory holdings • public relations • ex gratia payments.