two ways :: one outcome

Risk Management Policy and Framework

December 2014

Central Desert Regional Council

phone 1300 360 605

08 89589500

email info@centraldesert.nt.gov.au

location 1Bagot Street Alice Springs NT 0870

post PO Box 2257 Alice Springs NT 0871

web www.centraldesert.nt.gov.au

Release Notice

File name:	2014 Risk Management Policy and Framework v2.doc
Author:	Edward Fraser – Director Finance and Corporate Services
Reason for release:	The following document has been developed by the Central Desert Regional Council as part of its Risk Management Framework.
Contact information:	For further information please contact:
	Edward Fraser <u>Director Finance and Corporate Services</u>
	Central Desert Regional Council PO Box 2257, Alice Springs, NT 0871 1 Bagot Street, Alice Springs, NT, 0870 Tel/Direct: (08) 8958 9531 | Fax: (08) 8958 9501 Mobile: 0417 392 157 edward.fraser@centraldesert.nt.gov.au
Reference Number:	P32
Organisational Unit:	ALL
Responsible Position:	Chief Executive Officer
Relevant Delegations:	Not Applicable
Date Adopted:	5th December 2014
Review Date:	Every two years

Contents

Release Notice.. 2

1 Introduction 4

2 Risk Management Policy 5

2.1 Policy Statement 5

2.2 References 5

2.3 Scope 5

2.4 Objectives 5

3 Risk Management Framework 6

3.1 Definitions 6

3.2 Key Risk Management Principles 6

3.3 Key Outcomes 6

3.4 The Risk Management Process 7

3.5 Main Elements of the Risk Management Process 7

3.5.1 Establish the context 7

3.5.2 Identify the risk 7

3.5.3 Analyse risk 7

3.5.4 Evaluate risk 8

3.5.5 Treat risks 8

3.5.6 Monitor and review 8

3.5.7 Communicate and consult 8

3.6 Applying the Risk Management Process 8

3.7 Risk Management Methodology 8

3.8 Risk Management Framework 8

3.9 Responsibility and Accountability of the Risk Manager 9

3.10 Responsibility and Accountability for Risk Management 10

3.11 Risk Identification 11

Appendix A: Risk Management Context 12

Appendix B: Risk Assessment Criteria 14

Figures

1 Introduction

Risk management involves managing to achieve an appropriate balance between realising opportunities for gains while minimising losses. It is an integral part of good management practice and is an essential element of good corporate governance. It is an iterative process consisting of steps that, when undertaken in sequence, enable continuous improvement in decision-making and facilitate continuous improvement in performance.

In this document, the Central Desert Regional Council establishes the processes by which it will manage its risks. The Council has utilised the approach established in the AS/NZS 31000:2009 Australian Standard and adopts this as its basic approach to risk management. According to the standard, in order for a risk management approach to be effective a framework should be established that integrates the process for managing risk into the organisation's overall governance, strategy and planning, management, reporting processes, policies, values and culture. This document assists in this process.

The management of risk within the Council should assist by:

- Increasing the likelihood of achieving objectives;
- Fostering a culture of proactive management;
- Increasing awareness of the need to identify and treat risk throughout the organisation;
- Improving the identification of opportunities and threats;
- improving financial reporting;
- improving governance;
- improve stakeholder confidence and trust;
- establish a reliable basis for decision making and planning;
- improving operational effectiveness and efficiency;
- enhancing health and safety performance as well as environmental protection;
- improving loss prevention and incident management;
- minimising losses; and
- improving the Council's resilience.

2 Risk Management Policy

2.1 Policy Statement

The Central Desert Regional Council is committed to managing risk in the Council and will implement the AS/NZS 31000:2009 Australian Standard as the minimum standard. It is understood by the Council that Risk Management is the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, and analysing, evaluating, treating, monitoring and communicating risk.

The Executive Management Team (EMT) is responsible for developing a Risk Management Plan for the Council. The Council recognises that adequate resources are needed to implement the risk management program. The EMT are to ensure that all of the risk management processes are fully documented and managed through the records management system.

2.2 References

The reference documents used for this Policy and Framework are the Australian and New Zealand Standard AS/NZS 31000:2009 - Risk Management Principles and Guidelines and HB4360:2004 - Risk Management Guidelines.

2.3 Scope

This policy covers all the operations of the Council, including corporate governance, strategic planning, internal and external communications, information technology, resource management financial and human resources as well as operational risks such as legal compliance, business risks, tenders and contract management, project management, asset management, infrastructure management and emergency preparedness and response.

2.4 Objectives

The objectives of the risk management framework are to:

- To implement Risk Management Standard AS/NZS 31000:2009.

- To define the Council's tolerance to risk and communicate it throughout the Council.

- To communicate with the community about the Council's approach to risk.

- To protect the reputation of the Council.

- To develop a Risk Management Plan that is aligned to the Strategic Planning process.

3 Risk Management Framework

3.1 Definitions

Risk can be defined as the combination of the probability of an event and its consequences. In all types of undertaking, there is the potential for events and consequences that constitute opportunities for benefit (upside) or threats to success (downside).

Risk management is the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.

The **risk management process** is the systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, and analysing, evaluating, treating, monitoring and communicating risk.

3.2 Key Risk Management Principles

The following risk management principles are applied throughout:

- identify and rank all significant strategic, operational, special project, tender and contract and new service risks using the Central Desert Regional Council risk management process;

- ensure risk management becomes part of day-to-day management;

- provide staff with the policies and procedures necessary to manage risks;

- ensure staff are aware of risks and how to manage them; and

- monitor the Council's strategic risk profile and implement a continuous improvement approach to risk management.

3.3 Key Outcomes

Risk management consists of a systematic process which incorporates identifying, assessing and then dealing with, or otherwise managing, risk.

The key outcomes of managing risk include:

- Maximising opportunities by more effective budget and day to day operational planning;

- Increased knowledge and understanding of key strategic and operational risk exposures;

- Fewer costly surprises, for example by increasing the ability to prevent adverse outcomes;

- Better outcomes in terms of organisational efficiency and effectiveness; and

- Greater transparency in decision-making and the ongoing control of processes.

3.4 The Risk Management Process

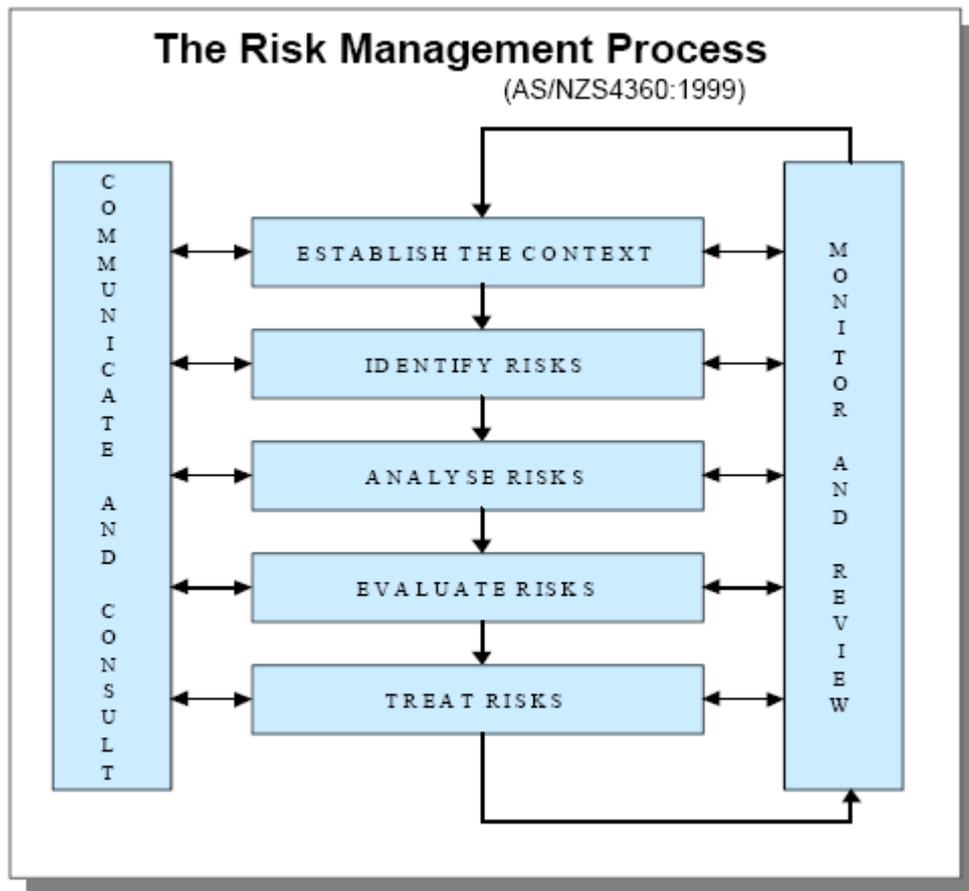The key elements of the risk management process are set out in Figure 1 below:

Figure 1: Key Elements of the Risk Management Process

3.5 Main Elements of the Risk Management Process

3.5.1 Establish the context

Establish the strategic, organisational and risk management context in which the rest of the process will take place. Criteria against which risks will be evaluated should be established and the structure of the analysis identified.

3.5.2 Identify the risk

Identify what why and how things can arise as the basis for further analysis or scenario planning.

3.5.3 Analyse risk

Determine the existing controls and analyse risks in terms of consequence and likelihood in the context of those controls. The analysis should consider the range of potential consequences and how likely those consequences are to occur. Consequences and likelihood may be combined to establish an estimated level of risk.

3.5.4 Evaluate risk

Compare estimated levels of risk against the pre-established criteria. This enables risk to be ranked so as to identify management priorities. If the levels of risk established are low, then risks may fall into an acceptable category and treatment may not be required.

3.5.5 Treat risks

Accept and monitor low priority risks. All risks will be reviewed, however, usually only extreme or high risks will be treated.

3.5.6 Monitor and review

Monitor and review the performance of the risk management system and changes which might affect it. The Audit and Risk Committee will play a big role in reviewing and monitoring the risk management approach.

3.5.7 Communicate and consult

Communicate and consult with internal and external stakeholders as appropriate at each stage of the risk management process and concerning the process as a whole.

3.6 Applying the Risk Management Process

The Central Desert Regional Council uses the Australian/New Zealand Risk Management Standard AS/NZS 31000:2009 as a guide for its applying the risk management process.

The Council uses its electronic records system to record and document the risks and treatment/action plans to support the risk management process.

3.7 Risk Management Methodology

The Central Desert Regional Council risk management methodology is consistent with the Australian Risk Management Standard and involves:

- Developing an understanding of the organisational context, including its strategic goals, its business functions and processes, and resources and stakeholders involved in achieving its objectives;

- Conducting a process of identifying the risks to which business operations and resources are exposed;

- Assessing for each risk the likelihood and consequence of an occurrence, the resources involved, and the effectiveness of risk mitigation and control;

- Recording and assessing specific consequences and controls;

- Developing an action plan for each 'Extreme' or 'High' level risk, identifying risk treatment options such as reducing the likelihood and/or consequence, avoiding, transferring, accepting, or otherwise treating the risk;

- Ongoing monitoring and review; and

- Communicating and consulting at all stages of the process between all levels of management and staff.

3.8 Risk Management Framework

The key elements of the risk management framework are set out in Figure 2 below:
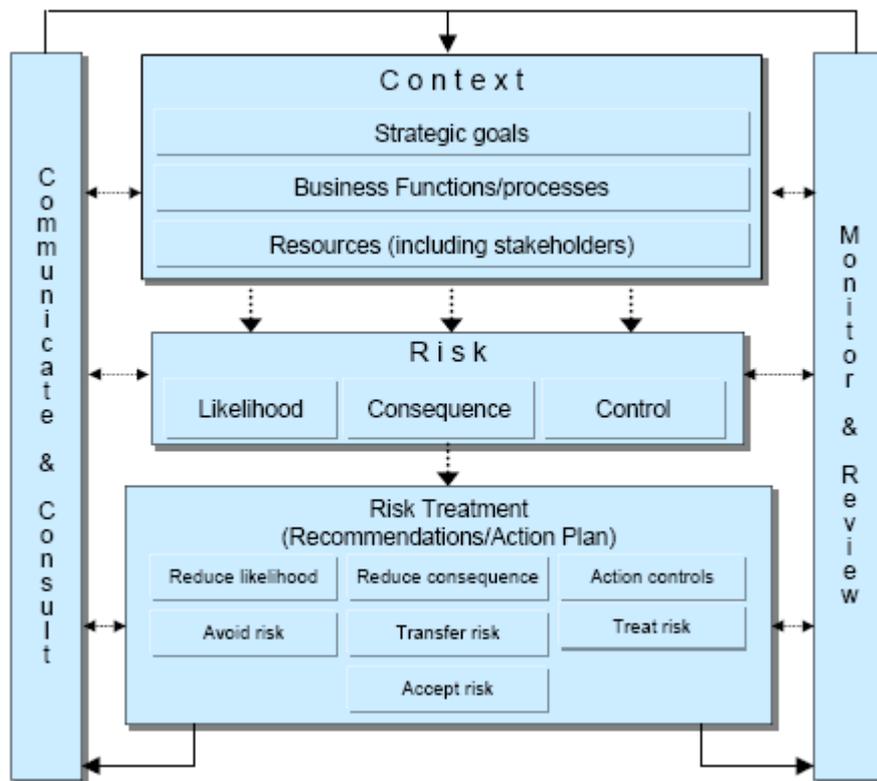
Risk Management Framework

Figure 2: Risk Management Framework

3.9 Responsibility and Accountability of the Risk Manager

For the purposes of this policy the Director Finance and Corporate Services has been designated as the risk manager.

It is the responsibility of the risk manager to provide advice, facilitation, co-ordination, guidance and assistance to management and staff to implement each of the following steps:

- Develop the Risk Management Policy statement
- Determine and define the linkages between the business and the risk management policy and objectives
- Determine and define risk evaluation criteria
- Establish the framework and responsibilities for the implementation of the risk management system
- Prepare, update and maintain a risk register that becomes the Annual Risk Management Plan.
- Review the linkages to the insurance program
- Ensure that the framework is adopted and maintained.

3.10 Responsibility and Accountability for Risk Management

Elected members are responsible for:

- Ensuring that a Risk Management Policy has been developed, adopted and communicated throughout the Council.

- Ensuring that the CEO has implemented the Risk Management Standard AS/NZS 31000:2009.

- Reviewing the Risk Management Policy.

- Annual performance review of the risk management implementation with the CEO.

Audit and Risk Committee members are responsible for:

- Monitoring and review of Risk Management Plan

- Review of the Risk Management Policy

CEO and Executive are responsible for:

- The full implementation of AS/NZS 31000:2009 tailored to all directorates.

- Establishing the risk tolerance level of the Council for adoption by the Council.

- Developing and managing the risk management plan for the Council.

- Ensuring that risk management is a standard agenda item for all executive management meetings.

- The Executive also meet and form the Risk Management Committee.

Risk Management Committee are responsible for:

- Communicating the risk management plan for the Council, the policy to all employees and displaying a copy of the policy on staff notice boards and intranet.

- Development of Risk Management skills through training and education.

- Establishing and maintaining the Risk Management Plan.

- Ensuring that all risk management processes are fully recorded throughout the Council.

Managers and Coordinators are responsible for:

- Identifying and measuring performance indicators for risk management that cascade from the risk management plan to position descriptions and performance appraisals.

- Ensuring that Risk Management is a standard agenda item at all meetings including toolbox meetings.

- Identifying and assessing all the potential risks in their area of responsibility.

- Collating, assessing, treating and reporting to the Risk Management Committee of all areas and tasks under their responsibility.

Employees are responsible for:

- Complying with the Council's risk management policy and procedures.

- Attending risk management training.

- Actively participating in the risk management program and organisational performance review and evaluation program.

- Actively participating in the Council's continuous improvement program

3.11 Risk Identification

Risk identification sets out to identify the Council's exposure to uncertainty. This is achieved by understanding the organisation, the context in which it operates, the legal, social, political and cultural environment in which it exists, as well as the considering the Council's strategic and operational objectives, including factors critical to its success and the threats and opportunities related to the achievement of these objectives.

Risk identification will be approached in a methodical way to ensure that all significant activities within the organisation have been identified and all the risks flowing from these activities defined. All associated volatility related to these activities should be identified and categorised.

The risk identification process will be conducted against the following a range of risk categories:

- *Strategic - These risks concern the long-term strategic objectives of the Council. They can be affected by such areas as resource availability, political risks, legal and regulatory changes, reputation and changes in the physical environment.*

- *Operational - These risks concern the day-today issues that the Council is confronted with as it strives to deliver its strategic objectives.*

- *Financial - These risks concern the effective management and control of the finances of the organisation and the effects of external factors such as revenue raising capability, grant dependence, interest rate movement and other market exposures.*

- *Compliance - These risks concern such issues as legislative compliance, health & safety, environmental, employment practices and other regulatory issues.*

These are further elaborated in Appendix A.

Whilst risk identification can be carried out by outside consultants, the Council will conduct risk identification workshops in-house as much as possible.

Appendix A: Risk Management Context

Strategic Risk

- **Failure to achieve objectives**

  Strategic risk is based on the strategic environment and the failure of the organisation to achieve its stated goals and objectives, for example, as documented in its strategic and business plans (vision, mission, strategy, key performance indicators, etc)

Operational Risks

- **Asset management, development and maintenance risk**

  Risk areas addressed within this section include the management/safeguarding of property and assets; including the maintenance and development of new/existing sites and facilities and the purchase/maintenance operational equipment and supporting resources.

- **Legal, contractual and regulatory risk (including compliance and liability)**

  Includes consequential loss, non-compliance with legislative and regulatory requirements, procurement, conduct of tender processes, corporate governance, accountability mechanisms, management of contracts, non-compliance with contract terms and conditions and public liability.

- **Finance and economic risk**

  Income stream, credit risks, maintenance and growth of revenue streams, fraud and corruption control, and delays in receiving projected revenue.

- **Human resources risk**

  This includes safety, staff morale and industrial relations issues in relation to the organisation, its staff, customers, contractors and the public.

- **Reputation and image risk (involving stakeholders, staff, customers and the public)**

  This includes the political and community profile, the media and media coverage of the organisation.

- **Political and change risk**

  This includes political decisions that influence the operations of the organisation ('stroke of a pen' risk), key political appointments that influence the organisation, liaison with key stakeholders and the community.

- **Environmental risks**

  Contamination, spills, noise, water and air pollution that affect the organisation, its customers, staff, contractors or the public, either due to accident, inadvertent or deliberate action(s), or negligence.

- **Technology and information risks**

  Includes the application, obsolescence or change in technology solutions affecting the organisation's business. Also the security, integrity, availability, confidentiality, management and storage of information, in both electronic and paper form, as well as intellectual property issues including ownership, loss, theft, unauthorised disclosure, abuse and infringement.

- **Business interruption and natural disaster risk**

  Ability of the organisation to maintain its business following a major incident such as the loss of a major facility (i.e. Administration Building), operation, system, key personnel team or team member, or following a major natural disaster or other incident affecting the organisation, its facilities, staff, customers, service providers, suppliers, contractors or other stakeholder dependencies).

Appendix B: Risk Assessment Criteria

Risk Rating - Likelihood Definitions

Rating	Key Word / Descriptor	Description	Frequency
1	Rare	May occur but only in exceptional circumstances	1 in 10,000 - 100,000 Less than once in fifteen years
2	Unlikely	Could occur at some time	1 in 1,000 to 10,000 At least once in 10 years
3	Possible	Should occur at some time in the future	1 in 100 - 1,000 At least once in three years
4	Likely	Will probably occur in most circumstances	1 in 10 - 100 At least once a year
5	Almost Certain	Is expected to occur in most circumstances	> 1 in 10 More than once a year

Risk Rating - Consequence Definitions

Rating	Key Word/ Descriptor	Financial – refers to core funding	Operation	Reputation	People / Health	Environmental Impact	Cultural
1	Insignificant	< $20,000	Little impact	Unsubstantiated, low impact, low profile or no news item	No injuries or ailments requiring medical attention	Brief pollution but no environmental harm	Unsubstantiated transgression of cultural protocol
2	Minor	$20,000 to	Inconvenient	Substantiated, low impact,	Minor injury or first aid	Minor/ transient	Minor transgression of

		$100,000	delays	low news profile	treatment cases	environmental harm	cultural protocol resulting in low level discomfort.
3	Moderate	$100,000 - $250,000	Significant delays to major deliverables	Substantiated, public embarrassment, moderate impact, moderate news profile	Serious injury causing hospitalisation or medical treatment cases	Significant environmental harm with mid term recovery	Interference with cultural event or practice. Temporary impact on sacred site. Temporary disengagement with community.
4	Major	$250,000- $500,000	Non achievement of major deliverables	Substantiated, public embarrassment, high impact, high news profile, third party actions	Death or life threatening injury or multiple serious injuries causing hospitalisation	Significant long term environmental harm	Desecration of sacred site or major interference with significant cultural event. Disengagement with the community.
5	Catastrophic	More than $500,000	Non achievement of key objectives	Substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile, third party actions	Multiple deaths or multiple life threatening injuries or severe permanent disabilities	Catastrophic, long term environmental harm	Permanent desecration or destruction of significant sacred site. Total permanent loss of cultural expression. Total or permanent disengagement with the community.

RISK DEFINITION AND CLASSIFICATION

E – Extreme risk – detailed action plan required
H - High risk – needs senior management attention
M – Medium risk – specify management responsibility
L – Low risk – manage by routine procedures

High or Extreme risks must be reported to Senior Management and require detailed treatment plans to reduce the risk to Low or Medium.

		Consequence				
		Cultural	Unsubstantiated transgression of cultural protocol.	Minor transgression of cultural protocol resulting in low level discomfort.	Interference with cultural event or practice. Temporary impact on sacred site. Temporary disengagement with community.	Desecration of sacred site or major interference with significant cultural event. Disengagement with the community.	Permanent desecration or destruction of significant sacred site. Total permanent loss of cultural expression. Total or permanent disengagement with the community.
		Environmental Impact	Brief pollution but no environmental harm	Minor/ transient environmental harm	Significant environmental harm with mid term recovery	Significant long term environmental harm	Catastrophic, long term environmental harm
		People/Health	No Injuries or ailments requiring medical treatment.	Minor injury or First Aid Treatment Case.	Serious injury causing hospitalisation or medical treatment cases.	Death or life threatening injury or multiple serious injuries causing hospitalisation.	Multiple deaths or multiple life threatening injuries or severe permanent disabilities.
		Reputation	Unsubstantiated. Low impact, low profile or no news item	Substantiated, low impact, low news profile.	Substantiated, public embarrassment, moderate impact, moderate news profile.	Substantiated, public embarrassment, high impact news profile, third party actions.	Substantiated, public embarrassment, very high multiple impacts, high widespread multiple news profile, third party action.
		Operation	Little impact	Inconvenient delays	Significant delays to major deliverables	Non achievement of major deliverables	Non achievement of key objectives
		Financial	<$20,000	$20,000 to $100,000	$100,000 to $250,000	$250,000 to $500,000	More than $500,000

			Insignificant	Minor	Moderate	Major	Catastrophic
Probability:	**Historical:**		**1**	**2**	**3**	**4**	**5**
>1 in 10 More than once a year	Is expected to occur in most circumstances.	**5** Almost Certain	M	H	H	E	E
1 in 10 - 100 At least once a year	Will probably occur in most circumstances.	**4** Likely	M	M	H	H	E
1 in 100 – 1,000 At least once in three years	Should occur at some time in the future.	**3** Possible	L	M	M	H	E
1 in 1,000 – 10,000 At least once in 10 years	Could occur at some time.	**2** Unlikely	L	M	M	H	H
1 in 10,000 – 100,000 Less than once in fifteen years	May occur but only in exceptional circumstances.	**1** Rare	L	L	M	M	H

Likelihood (row label)

Risk evaluation of treatment options - Decision making issues

Acceptability	Is the treatment option likely to be accepted by relevant stakeholders?
Administrative efficiency	Is the treatment option easy to implement or will it be neglected because of difficulty of administration or lack of expertise?
Compatibility	How compatible is the treatment with others that may be adopted?
Continuity of effects	Will the effects be continuous or only short term? Will the effects of this option be sustainable? At what cost?
Cost effectiveness	Is it cost effective, could the same result be achieved at lower cost by other means?
Economic and social effects	What will be the economic and social impacts of this option?
Effects on the environment	What will be the environmental impacts of this option?
Equity	Are the risks and benefits distributed fairly e.g. do those responsible for creating the risk pay for its reduction?
Individual freedom	Does this option deny any basic rights?
Jurisdictional authority	Does this level of organisation or government have the authority to apply this option? If not, can higher levels be encouraged to do so?
Leverage	Will the treatment options lead to additional benefits in other areas?
Objectives	Are organisational objectives advanced by this option?
Regulatory	Does the treatment (or lack of treatment) breach any regulatory requirements?
Political acceptability	Is it likely to be endorsed by the relevant government authority? Will it be acceptable to communities?
Risk creation	Will the option introduce new risks?
Timing	Will the beneficial effects be realised quickly?