Policy

CORPORATE RISK POLICY

COUNCIL COMMITTEE:	Audit and Risk Subcommittee
RESPONSIBILITY:	Chief Executive
ADOPTED:	27 June 2019
REVIEW:	Every three years or as required
CONSULTATION:	Consultation is not required, per s.78, Local Government Act 2002.
RELATED DOCUMENTS:	Local Government Act 2002

Policy Objective

This Ashburton District Council (ADC) risk management policy provides the context and framework for how risks to ADC are to be managed.

The objective of the risk management process is to identify realistic possible risks faced by Council, analyse and evaluate these risks. The outcome of this evaluation is to be used to:

- Emphasise the importance of continuing to provide Council's core services and manage inherent risks

- Continually identify improvements required to Council services to avoid risk events, or minimise their impact or to realise identified opportunities

This policy defines the responsibilities of Council managers and staff to form and maintain the framework, and use it to make sound decisions in alignment with business objectives.

The main objectives of the Corporate Risk Policy are to:

- Record and maintain a risk management framework aligned with the AS/NZS ISO 31000:2009 standard;

- Define the roles of staff and managers within the risk management framework;

- Enhance ADC's ability to achieve business objectives and deal successfully with risks and issues as they occur

- Maintain the integrity of services

- Safeguard assets, people, finances and property

- Identify opportunities to reduce risk

- Create a culture where all employees accept responsibility for managing risk

- Demonstrate transparent and responsible risk management processes which align with and demonstrate good governance

- Utilise risk management process outputs as inputs into Council decision-making processes

Definitions

A **Risk** is defined in AS/NZS ISO 31000:2009 – *Risk management – Principles and guidelines,* as:

"Effect of Uncertainty on Objectives"

Effect: Deviation from the expected – positive or negative.

Objectives: Can have different aspects (see *Risk Types*) and can apply at different levels (see *Risk Hierarchy Levels*).

Risks: Often characterised by reference to potential events and consequences, and is often expressed in terms of a combination of the consequences of an event and the associated likelihood.

Uncertainty: The state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.

Risk Attitude

Risk Attitude is defined in AS/NZS ISO 31000:2009 – *Risk management – Principles and guidelines,* as the:

Organisation's approach to assess and eventually pursue, retain, take or turn away from risk
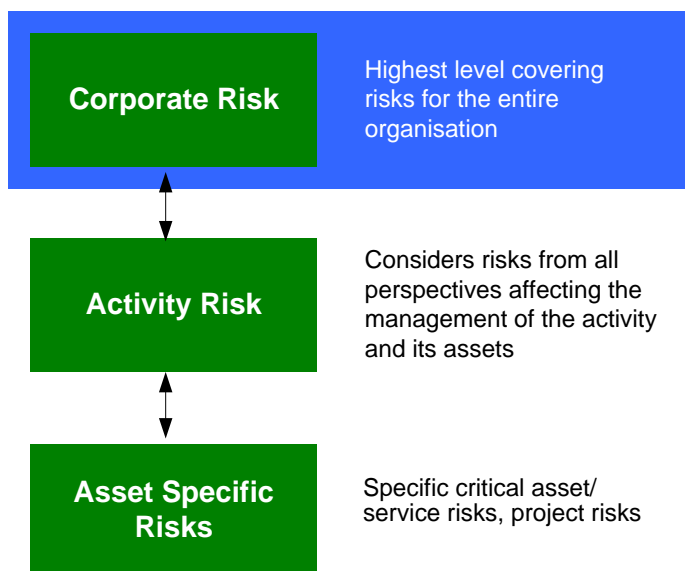
In defining ADC's risk attitude and determining the acceptable level of risk, Council will consider the following questions:

- What is the communities attitude to a loss of level of service?
- What time and resources are Council willing to commit to minimise risk exposures?
- What level of risk requires immediate action?
- What level of risk requires a formal response strategy to avoid the risk event or minimise its impact?
- What events have actually occurred in the past, at what level were they managed, and what were the impacts?
- Is Council comfortable with current risk levels, or do they feel they are taking too many, or not enough, risks?
- What are the consequences of not mitigating the risk?

Risk Hierarchy Levels

Risks are identified and managed at different levels in the organisation in line with the responsibilities, abilities and skills of the staff, and the specific nature of many key risks.

Figure 1 - Risk Hierarchy Levels

Corporate Risk	Highest level covering risks for the entire organisation
Activity Risk	Considers risks from all perspectives affecting the management of the activity and its assets
Asset Specific Risks	Specific critical asset/ service risks, project risks

Corporate Risks

Corporate risks are identified and managed by senior management (i.e. Chief Executive and Leadership Team). The focus of corporate risks is more likely, but not exclusively, to be on:

- External influences affecting Council's effective operations

- Risks that are common to more than one activity

- Risks around the Council's ability to meet service levels, react to emergencies, support the activities or specific projects

- The most critical activities and specific risks.

Corporate risks will also summarise or combine a number of Activity or Specific Risks (e.g. inadequate project management). These risks can be evaluated for each activity and the combined results used to form a corporate risk view.

Activity Risks

Activity Risks are pertinent to both a higher, corporate level, and to a more detailed asset –specific level. They may reflect corporate level risks applied specifically to the activity (e.g. lack of resources in the activity, impact of IT failure on the activity). Activity Risks may require more specific risk analyses to better quantify the actual risk faced.

Activity risks are best identified and managed by Activity and Asset Managers and their teams. The focus of activity risks is more likely, but not exclusively, to be on external and corporate influences impacting the activity, risk events that impact on operational efficiency, meeting standards and

expectations, promoting innovation and improvements, and specific risks affecting the most critical activities and assets.

Asset Specific Risk Analysis

Specific Risk Analyses might be carried out as a legislative requirement (e.g. water supply public health risk management plan), or because a more detailed risk analysis is required due to the potential to impact risks identified at the Activity or Corporate level (e.g. high cost/profile projects, activities critical to upkeep or restoration of service levels, or important to the minimisation of a major or catastrophic risk event.). The risks may also be of a short-term nature e.g. office relocation, infrastructure project, specific legislation introduction.

Risk Types

Risks events will derive from, or impact in one or more of the following ways. These are identified against each risk as *risk types*.

Community Safety

A risk event that adversely impacts on the health and safety of the community.

Operational

Risks affecting the efficient operation of ADC and the ability to function.

Reputation

Risks that affect the way Council and Council personnel are perceived:

- by the community
- by staff
- nationwide and internationally
- by stakeholders
- by the media

Financial

Risks related to the financial management of ADC and the ability to fund Council activities and operations now, and into the future, including risks resulting from an externally imposed economic environment.

Environmental

Potential or actual negative environmental or ecological impacts, regardless of whether these are reversible or irreversible in nature.

Our People

Risks related to staff; accidents, performance and engagement.

Legal

A risk event that results in ADC unknowingly or knowingly breaching statutes and stipulations, or exposed to liability.
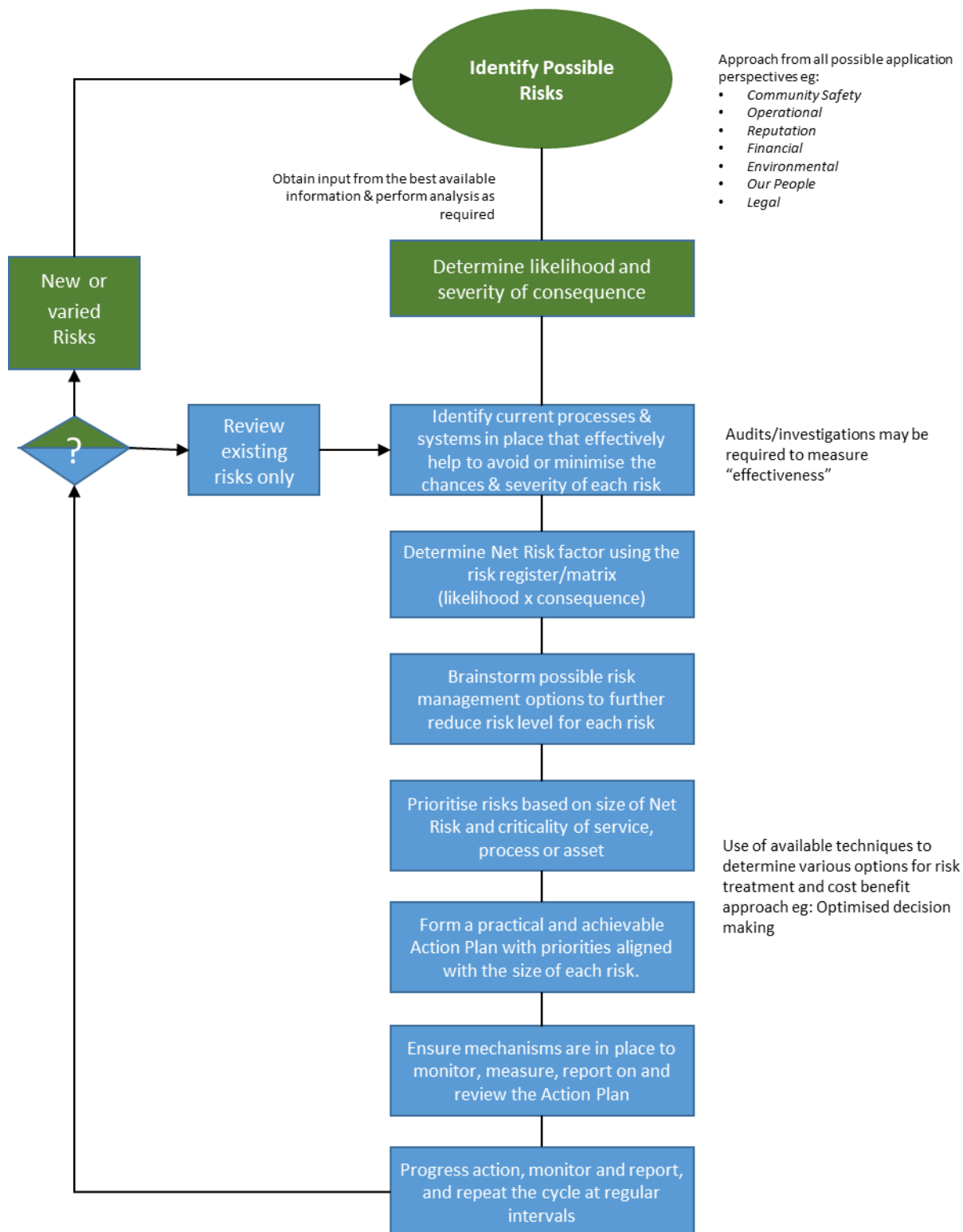
Responsibilities for Managing Risk

Position	Roles and Responsibilities
Council	• To obtain assurance that appropriate risk governance and management frameworks are in place, that Council decisions take risk into account appropriately, and that risks are being appropriately managed in the achievement of Council's objectives.
Audit and Risk Subcommittee	• To review and recommend approval of risk management frameworks, risk-related policies, the Risk Register, and review risk treatment options for critical risks.
	• To provide elected member input into setting the overall risk attitude, via recommendations to Council in respect of risk management frameworks, the Risk Register, and risk-related policies.
Chief Executive (CE)	• To grant management approval of the risk management framework and recommend it to the Audit and Risk Subcommittee.
	• To report critical risks to Council with treatment options.
	• To implement the risk management framework across the organisation and review for continuous improvement.
	• To lead and promote a risk-aware culture across the organisation.
Leadership Team (LT)	• To endorse the risk management framework and promote a risk-aware culture across the organisation.
	• To monitor the effective implementation of the risk management framework across the organisation and its integration with Council policies, processes and practices.
	• To receive and review the risk register, risk management policies, activity and asset management plans, and other risk-related reports on a regular or as-required basis.
	• To ensure new risks are processed (i.e. first receiver of new risks and consideration of these).
	• To facilitate the management of organisation-wide risks (including allocation of responsibility for organisation-wide risks) and risk management training.
Group Managers	• To implement the risk management framework within their Group.
	• To lead and promote a risk-aware culture across their Group.
	• To monitor the effective implementation of the risk management framework across their Group.
	• To facilitate the management of Group-wide risks (including allocation of responsibility for Group-wide risks)
Group Manager Business Support	• To manage the maintenance of the risk management framework.
	• To facilitate the ongoing review of the Risk Register.
	• To advise, or secure advice, on potential risk treatment for identified risk
	• To ensure integration of the risk management framework and risk management principles with Council policies, processes, and practices (including decision-making processes).
	• To challenge, where necessary, the risks, controls, mitigations, and accountabilities included (or not included) in the Risk Register, activity or asset management plans and other risk-related reports.
Activity / Asset	• To Include activity-related risks and controls in activity management plans and asset

Managers	management plans
	• Review and manage activity-related risks on an ongoing basis
	• To report high and critical risks to the Leadership Team with a recommended treatment plan
Risk Owners	• To support risk management of ADC within their sphere of delegated responsibility.
	• To ensure ongoing identification and assessment of risks, and responding appropriately relative to delegated responsibilities.
	• To manage the relevant risk, within acceptable risk tolerance levels
All Staff	• To maintain awareness of risks, risk management, and process
	• To undertake everyday identification and management of risks and improvement actions to minimise risk events and impacts

Risk Management Process

The following flowchart and text details the key elements of the Risk Management Process undertaken. The risk criteria and matrices have been proposed as the basis for risk evaluation in this section developed in line with the AS/NZS ISO 31000:2009 international risk standard.

Figure 2: Risk Management Process

Identify Possible Risks

Approach from all possible application perspectives eg:
- *Community Safety*
- *Operational*
- *Reputation*
- *Financial*
- *Environmental*
- *Our People*
- *Legal*

Obtain input from the best available information & perform analysis as required

New or varied Risks

Determine likelihood and severity of consequence

?

Review existing risks only

Identify current processes & systems in place that effectively help to avoid or minimise the chances & severity of each risk

Audits/investigations may be required to measure "effectiveness"

Determine Net Risk factor using the risk register/matrix (likelihood x consequence)

Brainstorm possible risk management options to further reduce risk level for each risk

Prioritise risks based on size of Net Risk and criticality of service, process or asset

Use of available techniques to determine various options for risk treatment and cost benefit approach eg: Optimised decision making

Form a practical and achievable Action Plan with priorities aligned with the size of each risk.

Ensure mechanisms are in place to monitor, measure, report on and review the Action Plan

Progress action, monitor and report, and repeat the cycle at regular intervals

Ashburton
DISTRICT COUNCIL

The following sections expand upon the risk management process as identified in the flowchart (previous page). The risk assessment process has been generally based upon the AS/NZS ISO 31000:2009 international risk standard to establish a Risk Matrix. This matrix provides a tool to quantify a risk by identifying the likelihood of the risk occurring and the outcomes, or consequences should the risk occur. The first step in the process is to identify the risks.

Identify Risks

All practically possible risks affecting the Council need to be identified. Risks can include the types quoted previously i.e. financial, operational, health and safety etc. Once identified, risks are entered into the risk register. The register is used to record and summarise each risk and to outline current mitigation measures and potential future management options.

The risk register can exist as an electronic document (e.g. in Word or Excel) and possibly in hard copy. This is to be maintained by the Group Manager Business Support.

Assessment of Risk Ratings

This policy is framed on the basis of "net risk" which is the potential harm created by a risk when all risk controls work successfully. "Net risk" is sometimes also referred to as "residual risk".

Net Risk = (likelihood – impact of controls) X (consequence – impact of controls)

This is a three-part process, with the final outcome being a risk rating for each risk. The risk rating enables prioritisation between those risks that are critical and those that are of a lesser nature.

Determining Likelihood and Consequence

Table 1 and Table 2 demonstrate the scales used to determine the likelihood and consequence levels, which are input into the risk calculation to consider the effect of a risk event.

The likelihood of occurrence and severity of consequences should be based on as much real data as possible, for example local knowledge or recorded events such as maintenance records, weather events etc. Some analysis may be required for verification. As Council is applying a "Net Risk" approach, the overall score for Likelihood must also reflect how **both** the existing controls in place **and** their current level of effectiveness impact to reduce the likeliness of occurrence. As much as practicable, allowance for the effects of controls on the likelihood of an event occurring should also be based on real data. It is important not to understate the likelihood of risk by assuming that all preventative controls are working successfully. Real data should also consider, wherever possible, the efficacy of current controls.

The likelihood scales identify how likely, or often, a particular event is expected to occur, these are shown in Table 1 below. The descriptors are there not as mandatory category requirements, but as a guide to assist ranking the probability in line with the nature of each risk.

Table 1: Likelihood of Occurrence		
Likelihood	**Rating**	**Descriptor** (example frequencies)
Rare	1	May occur only in exceptional circumstances e.g. once in 10 years
Unlikely	2	Could occur only very occasionally e.g. 2-3 out of every 10 years
Possible	3	Might occur from time to time e.g. 5 out of every 10 years
Likely	4	Will probably occur often e.g. 7 out of every 10 years

Likelihood	Rating	Descriptor (example frequencies)
Almost Certain	5	Is expected to occur in almost all circumstances e.g. 9 out of every 10 years

The Consequence descriptors in Table 2 indicate the level of possible consequences for a risk.

The Consequence scales identify how large the impact from a risk may be. As noted with the likelihood scale, the descriptors are there as a guide. The purpose of the guidance is to assist ranking the probable consequences for each risk against one or more of the seven risk types, depending on how many are relevant to the risk under assessment.

The severity of consequences should also be based on as much real data as possible, for example known costs or harm or the experience of other communities or organisations experiencing this harm. Some analysis may be required for verification. As Council is applying a "Net Risk" approach, the overall score for Consequence given must also reflect how **both** the existing controls in place **and** their current level of effectiveness reduce the severity of those consequences. As much as practicable, allowance for the effects of controls on the severity of an event impact should also be based on real data. It is important not to understate the severity of risk by assuming that all controls are working successfully. Real data should also consider, wherever possible, the efficacy of current controls.

As many risks will generate consequences under multiple types of risk, the overall score will be the Consequence Rating associated with the highest scoring risk type. For example, a risk scoring as "Major" for Community Safety, may score only as "Moderate" for Financial, but the overall score will reflect the higher of these scores.

Table 2: Consequence Rating					
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Score	1	2	3	4	5
Community Safety	Low possibility of minor injury.	Minor injury to single person or confined to a localised area.	Moderate injury or illness, affecting some people in a localised area.	Some loss of life, serious injury or illness affecting people across the district.	Widespread loss of life affecting majority of the district.
Operational	No loss of operational capability or negative disruption to service levels.	Loss of operational capability in some areas and some disruption to service levels.	Serious loss of operational capability for over 1 week and disruption to service levels.	Serious loss of operational capability for over 2 weeks and major disruption to service levels.	Serious loss of operational capability for over 4 weeks and serious disruption to service levels.
Reputation	Negative feedback from individuals or small groups	Loss of confidence among sections of the community.	Manageable loss in community confidence.	Large loss in community confidence that will take significant time	Insurmountable loss in community confidence.

	Insignificant	Minor	Moderate	Major	Catastrophic
	in the community. Negative regional multi-media coverage for up to 2 days.	Negative multi-media national-wide coverage for 2 days.	Negative multi-media national-wide coverage for several days.	to remedy. Negative multi-media national-wide coverage for up to 2 weeks.	Negative multi-media national-wide coverage for up to 2 weeks +.
Financial	Loss to Council or damage to local economy of less than $50,000	Loss to Council or damage to local economy of $50-000, $250,000	Loss to Council or damage to local economy of $250,000 - $1,000,000.	Loss to Council or damage to local economy of $1-$10 million.	Loss to Council or in damage to local economy of $10 million or more.
Environmental	Localised, temporary adverse environment-al effects.	Localised, minor reversible adverse environmental effects.	Localised, medium- term reversible adverse environmental effects.	Widespread, long-term reversible adverse environmental effects.	Widespread, irreversible adverse environmental effects.
Our People	Nil. Permanent full time staff turnover less than 10% p.a. Disengaged responses in staff survey less than 10%	Injury with less than 2 weeks' time-off. Permanent full time staff turnover 10% to 15% p.a. Disengaged responses in staff survey between 10-20%	Injury with 2 weeks to 3 months' time-off. Permanent full time staff turnover 15% to 20% p.a. Disengaged responses in staff survey between 20-30%	Injury with 3+ months' time-off. Permanent full time staff turnover 20% to 30% p.a. Disengaged responses in staff survey between 30-50%	Loss of life. Permanent full time staff turnover exceeds 30% p.a. Disengaged responses in staff survey more than 50%
Legal	ADC sued or fined less than $50,000.	ADC sued or fined for between $50,000 and $250,000.	ADC sued or fined for between $250,000 and $1 million.	ADC sued or fined for between $1 - 10 million.	ADC sued or fined for more than $10 million.

As noted previously, some controls may not be working at their maximum effectiveness and there will be risks where, even with effective controls in place, net risk remains.

Overall Risk Rating

Table 3 shows how the scores for Likelihood and Consequence combine to give an overall risk rating.

Table 3: Risk Assessment Matrix

Consequence →					
	Insignificant	**Minor**	**Moderate**	**Major**	**Catastrophic**
Rare	1	2	3	4	5
Unlikely	2	4	6	8	10
Possible	3	6	9	12	15
Likely	4	8	12	16	20
Almost certain	5	10	15	20	25

(← Likelihood)

Table 4 describes each level of the overall risk rating. Having established the comparative risk level applicable to individual risks, it is possible to rank those risks. Five risk categories have been used: Critical, High, Medium, Low and Insignificant (see Tables 3 & 4).

Once the impact has been ranked according to the relative risk level it poses, it is then possible to target the treatment of the risk exposure, by beginning with the controls for critical risks. This work largely occurs at an activity level through Activity Management Plans.

Table 4: Comparative Levels of Risk

Critical Risk	**Immediate action required to reduce risk**
High Risk	**Senior management attention to manage risk**
Medium Risk	**Management responsibility must be specified and risk controls reviewed**
Low Risk	**Managed by a routine process**
Insignificant Risk	**Examine where un-needed action can be reduced**

Risk and Controls

Gross risk is the "unmanaged risk", being the level of risk that would exist if no controls were in place or controls that were in place were not working. We have streamlined our processes and do not calculate this risk, as we are not aware of any unmanaged risks within our operations, or any managed risks with completely dysfunctional controls.

Part of the process for risk assessment is to list all current controls used to manage risks, and to identify new controls or improvements that will improve the effectiveness and/or the efficiency of risk controls. Current, new or improved controls are listed for each risk in the Risk Register and these are prioritised for action in the Action Plan.

Assessment of costs and benefits for new and improved controls

At the implementation phase, Activity or Asset Managers assess the benefits and costs of new or improved controls, rather than just working down from the highest risk regardless of cost. For example:

- *A high risk may have to remain due to the prohibitive costs associated with avoidance or mitigation*
- *A medium risk event could be easily and cost-effectively avoided within resources available.*

Managers should also consider how the new or improved control fits within the overall business objectives of Council, and not from solely a risk management perspective. Wherever possible, new or improved controls should align with other actions to:

- Reduce capital investment costs
- Reduce operating and maintenance costs
- Reduce business risk exposure
- Increase effective asset life/value
- Increase level of service
- Promote greater environmental, social and cultural value (in addition to financial and economic benefit).

This deeper understanding of costs and benefits may result in a refined priority ranking for new and improved controls appearing in Activity or Asset Management Plans.

Resources for New and Improved Controls

It may be possible to implement improvements within existing operating and capital budgets. This should always be regarded as the first source for funding. Where additional resources will be required to implement new and improved controls, these must be reflected in budget proposals linked to the Asset or Activity Management Plan and subject to normal budget scrutiny and approval processes.

Risk Action Plan

Actions to implement new and improved controls to improve risk management are identified and prioritised in the Risk Action Plan which forms part of the Risk Register.
The Risk Action Plan will include information on:

- **Responsibility:** Person(s) responsible for ensuring actions are completed on time, within budget and to the required standard.
- **Timeframe:** Achievable target date to be monitored and reported against
- **Method and frequency of monitoring and reporting:** Progress against actions to control critical risks will be reported at least annually to Council by the Chief Executive via Audit and Risk Subcommittee. Progress against actions to control critical and high risks will be reported by Group Managers to the Leadership Team. Progress to control critical, high and medium risks will be reported by the Activity Manager to the relevant Group Manager.

The actions listed will be monitored and reviewed by the Leadership Team

Review of Risks

Most of the time, the risks identified will remain the same and reviews will occur in the context of those known risks. It is important to recognise that new risks may arise from time to time, or an existing risk may change materially. In these cases, risks should be reviewed.