Company Procedure

GOVERNANCE			
	Document No	:	CEOP0002.21
	Amendment No	:	0
	Approved By	:	CEO
	Approval Date	:	29/07/2014
	Review Date	:	29/07/2017

CEOP0002.21 RISK MANAGEMENT

1.0 PURPOSE

To articulate the company's risk management process, assessment methodology and reporting requirements.

2.0 SCOPE

This procedure has direct application to the management of material risks at a Corporate level and all or parts of this procedure have applicability to assist with risk management associated with:

- fraud and corruption;
- major business process change;
- major capital projects;
- asset management investment prioritisation;
- major IT projects;
- business continuity – Business Impact Assessments; or
- whenever there is a need to formally document the risks associated with one-off situations.

This procedure is not intended to replace established risk-based processes used to assess site or task specific risks, eg environmental site assessments, safety risks associated with tasks.

3.0 REFERENCES

Internal:
CECP0002 - Board Policy (Governance) – Governance
CECP0002.02 - Board Policy (Governance) – Compliance
CECP0002.03 - Board Policy (Governance) – Risk Management
CECP0002.06 - Company Policy (Governance) – Business Continuity Management
CEOP0002.20 - Company Procedure (Governance) – Changes to Risk Based Management Plans
CECM1000.02 - SSHE Manual: Risk Management
CEOF0002.23.01 - Company Form (Governance) – Risk Assessment Template
CEOF0002.23.02 - Company Form (Governance) – Change Management Risk Assessment Template
CEOF0002.23.03 - Company Form (Governance) – Risk Management Reporting Template
CEOF0002.23.04 - Company Form (Governance) – Emerging Risk Register
CEOM0002.24 - Risk Assessment Training Manual
Annexure A - Risk Management RACI Matrix

External:
Work Health and Safety Act 2011 (NSW)
AS Records classification handbook – HB5031 – 2011
NSW Treasury Risk Management Toolkit for the NSW Public Sector (TPP12-03)
ISO 31000:2009 – Risk Management – Principles and Guidelines
General Retention and Disposal Authority: Administrative Records GA28

4.0 DEFINITIONS

Where applicable, definitions are consistent with ISO 31000:2009 – Risk Management – Principles and Guidelines.

As Low As Reasonably Practicable (ALARP)
Core to this concept is “reasonably practicable”. The objective is to eliminate risk. If it is not reasonably practicable to eliminate a risk, then it should be minimised to as low as reasonably practicable (in accordance with the hierarchy of controls). ALARP is the level of risk that is tolerable and cannot be reduced further without the expenditure of cost, time and/or effort that is disproportionate to the benefit gained or where the solution is impractical to implement.

Bow-Tie Methodology
The Bow-Tie methodology is used to understand the control environment. It provides a graphical means to describe the relationship between hazards, hazardous events (centre), causes (left side) and consequences (right side). Barriers are used to display what measures an organisation has in place to control the risk.

Business Continuity Management (BCM)
Holistic management process that identifies potential threats to an organisation and the impacts to business operations those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability of an effective response that safeguards the interests of key stakeholders, reputation, brand and value-creating activities [ISO 22301].

Business risk category
Nine business risk categories have been identified for grouping high level risks that have the potential to prevent the company from achieving its objectives. A Risk Category Owner is assigned to monitor the risk management activities undertaken in regard to each business risk category.

Cause
A factor that could lead to the hazardous event occurring. For distinct hazardous events, causes need to have the ability to result in the hazardous event in their own right. Where hazardous events are stated in more general terms, the cause should be expressed in terms of a contributing hazardous event related to an activity.

Common Risk Matrix
The 5 x 5 matrix appended to the Board Policy Risk Management that is used to determine the risk rating for a particular combination of consequence and likelihood. The common Risk Matrix reflects the risk appetite approved by the Board.

Control
Measures that modify risk. Controls include policies, procedures, processes, devices, practices or other actions which modify risk. These may also be described as “barriers”.

Control environment
The combination of a suite of controls, (both prevention and mitigation) contained on a bow-tie in place to manage a risk.

Consequence
The outcome of an event affecting objectives.

Corporate Risk Management Plan
The Corporate Risk Management Plan details the risks to the achievement of the company’s strategic and operational objectives. This includes the company risk profile, results of the risk assessments, key risk indicators and the treatment action plans.

Divisional Governance, Risk & Compliance (GRC) Representatives
The Executive Leadership Team nominated representative that coordinates governance, risk and compliance related initiatives and reporting within each division.

Document Control
Employees who work with printed copies of documents must check the Business Management System (BMS) regularly to monitor version control. Documents are considered “uncontrolled if printed”, as indicated in the footer.

Escalation factor
See primary control defeating factor.

Escalation control
See supporting control.

Executive Leadership Group
Chief Executive Officer, Chief Operating Officers, Group Chief Financial Officer, Group Executive Network Strategy, Group Executive People & Services and Board Secretary.

Executive Leadership Team
Chief Operating Officer, General Manager Health, Safety & Environment, General Manager People & Services, Chief Engineer, General Manager Network Development, General Manager Network Operations, General Manager Finance & Compliance and General Manager Information, Communications & Technology.

External context
The external environment in which the company seeks to achieve its objectives. External context may include:

- cultural;
- social;
- political;
- legal;
- regulatory;
- financial;
- technological;
- economic;
- natural and competitive environment (whether international, national, regional or local);
- key drivers and trends having impact on the objectives of the company; and
- perceptions and values of external stakeholders.

Group Risk Category Owner
The Group Executive with the authority and accountability to undertake risk assessments to support the delivery of the Strategic Plans, and reviewing and endorsing the risk ratings and ALARP status of the hazardous events included in their risk category.

Hazard
Source of potential harm.

Hazardous event
An event which has the potential to cause harm (ie loss or damage).

Hierarchy of controls

Elimination of a hazard is the most effective control and if this is not reasonably practicable to achieve, implementation of additional controls should be considered based upon their degree of effectiveness. This order is referred to as the hierarchy of controls and comprises elimination, substitution, isolation, engineering controls, administrative controls and finally use of personal protective equipment.

Inherent risk

The inherent risk rating is based on the plausible worst case scenario assuming the absence of company established controls but with the presence of existing external controls such as regulations, road rules etc. and reliance on common sense.

Insurance

A contract in which the insurer agrees to compensate the insured (the company) for any losses or damages caused by risks identified in the contract.

Internal context

The internal environment in which the company seeks to achieve its objectives. Internal context may include:

- governance, organisational structure, roles and responsibilities;
- policies, objectives and the strategies that are in place to achieve them;
- the capabilities, understood in terms of resources and knowledge eg capital, time, people, processes, systems and technologies;
- information systems, information flows and decision making processes (both formal and informal);
- relationships with, and perceptions and values of internal stakeholders;
- the company’s culture;
- standards, guidelines and models adopted by the company; and
- form and extent of contractual relationships.

Key control

A control that lies directly on the path between a cause and a hazardous event and if not operating effectively, would result in a significantly weakened control environment. Key controls are a subset of primary controls and may be subject to more frequent monitoring and auditing due to their relative importance.

Key Risk Indicator (KRI)

An indicator used to monitor the effectiveness of the control environment and can be either active (leading) or reactive (lagging). Active indicators measure variables that are believed to be precursors of future risk management performance. Reactive indicators measure historical, after-the-fact performance to show when the desired outcome (in terms of controls) has not been achieved.

Likelihood

Chance of something happening.

Network Fatal Risk

A hazardous event that has the potential to result in a permanent disability or fatality. Network Fatal Risks are those that can be described as low frequency, however high consequence and form a prioritised subset of operational risks.

Operational Risk

A hazardous event linked to day-to-day activities undertaken by the company.

Positive risk culture
Is evident in a company when employees are aware of the company's activities, operations and objectives; consider the opportunities and what can go wrong; and takes action to harness the opportunities and address the consequences.

Primary control
A control that lies directly on the path between a cause and a hazardous event. It may or may not be a key control.

Primary control weakening factor
A condition that leads to increased risk by defeating or reducing the effectiveness of a primary control. When being considered as part of an incident investigation these may also be described as “contributory factors”.

Project Manager
The employee that leads a particular project and is responsible and accountable for completing the project on time and on budget in a safe and environmentally responsible manner.

Project/Program Sponsor
Manager or individual to whom the Project Manager is accountable.

Recordkeeping
Making and maintaining complete, accurate and reliable evidence of business transactions in the form of recorded information (Source: AS Records classification handbook – HB5031 – 2011).

Residual risk
The risk remaining after risk treatment. Also refers to the current level of risk taking into account the existing controls and their known level of effectiveness.

Responsible, Accountable, Consult, Inform (RACI) Matrix
A chart which describes the participation by various roles in completing tasks or deliverables for a project or business process.

Review date
The review date displayed in the header of the document is the future date for review of a document. The default period is three years from the date of approval however a review may be mandated at any time where a need is identified due to changes in legislation, organisational changes, restructures, occurrence of an incident or changes in technology or work practice.

Risk
The effect of uncertainty on objectives.

Risk analysis
The process to comprehend the nature of risk and to determine the level of risk. Risk analysis provides the basis for risk evaluation and decisions about risk treatment.

Risk appetite
The amount and type of risk that the company is willing to pursue, retain, take or turn away from risk. Refer to the risk criteria set out in Table 3.

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

Risk Category Nominated Lead
Generally a Divisional GRC Representative or other employee that has been nominated by the Executive Leadership Team member to assist in the implementation of the Risk Management Framework. There may be more than one Risk Category Nominated Lead nominated per division. The Risk Category Nominated Lead supports the Risk Category Owner as required with Business Risk Category reporting and the annual risk assessment refresh.

Risk Category Owner
The Executive Leadership Team member nominated by the Chief Operating Officer to have oversight of all hazardous events contained within a Business Risk Category.

Risk evaluation
The process of comparing the results of the risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable. Risk evaluation assists in the decision making about the ALARP status and risk treatment.

Risk identification
The process for finding, recognising and describing risks.

Risk management
Coordinated activities to direct and control the company with regard to risk.

Risk Management Framework
The set of foundation documents and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the company.

Risk management plan
A document that formally collates the results of risk assessments related to a specific set of objectives. This includes the risk ratings, key risk indicators and treatment action plans for the reduction of risk to a tolerable level.

Risk management process
The systematic application of management policies, procedures and practices to the activities of communicating, consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk Management Strategic Plan
The Risk Management Strategic Plan details the initiatives aimed at strengthening system weaknesses identified through the monitoring and review of the Risk Management Framework. Implementation of the Risk Management Strategic Plan aims to embed continuous improvement in the Risk Management Framework and its application. Covering a three year period, the Risk Management Strategic Plan is reviewed and revised annually.

Risk Owner
The employee with the authority and accountability to make decisions to treat, or not to treat a risk. Generally this is the Risk Category Owner, however it may be another Executive Leadership Team member with accountability for the management of the hazardous event and development and completion of treatment action plans. (For projects refer to the Project/Program Sponsor.)

Risk profile
The description of the company’s risks.

Risk register
A record of information about related identified hazardous events including descriptions, controls and risk ratings.

Risk treatment
The development and implementation of measures to modify risk. Defined in the Risk Management process as a Treatment Action Plan. Risk treatment measures may include:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk in order to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk with another party or parties (including contracts and risk financing); and
- retaining the risk by informed decision.

Risk tolerance
The company's readiness to accept a residual risk based on the effectiveness of the control environment or the planned risk treatment actions.

Strategic Risk
A hazardous event either related to the development of the Corporate strategy or the delivery of initiatives contained in Strategic Plans.

Subject Matter Expert
An individual with in-depth knowledge of the related business process/es.

Supporting control
A control that prevents a primary control weakening factor defeating or reducing the effectiveness of a primary control. It may also provide forewarning that control effectiveness is reduced.

Uncertainty
The state, even partial, of deficiency of information related to a future event, consequence or likelihood.

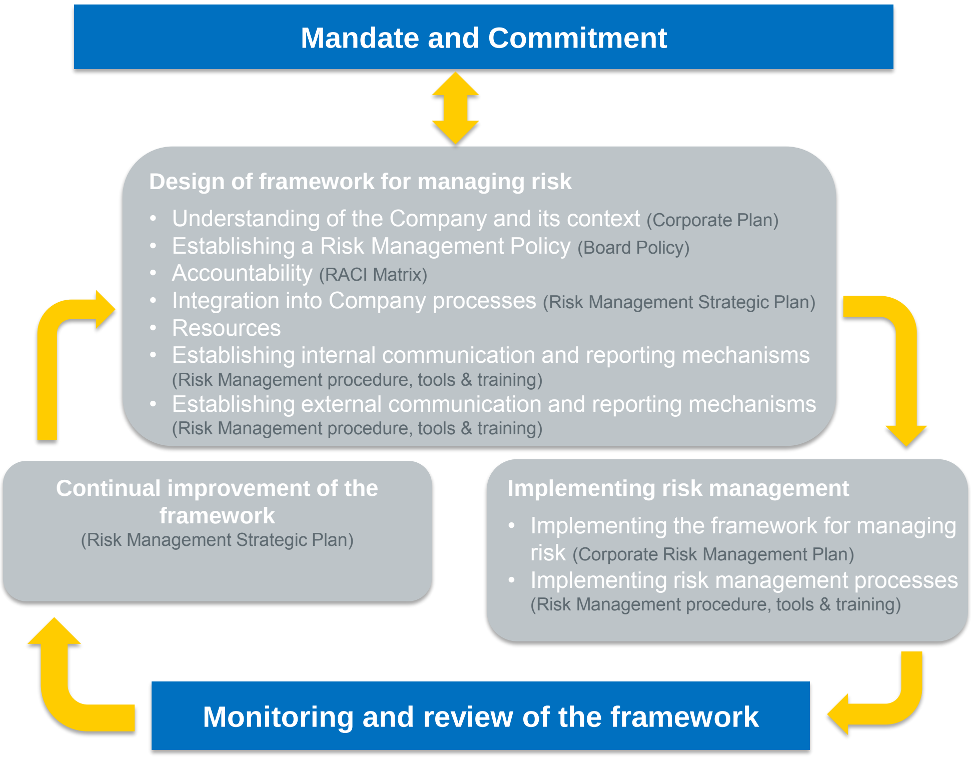
5.0 ACTIONS

5.1 Understanding the Risk Management Framework

The success of risk management depends on the effectiveness of the management framework providing the foundations and arrangements that will embed it throughout the company, at all levels. The framework assists in managing risks effectively through the application of the risk management process at varying levels and within specific contexts of the company. The framework allows for information about risk derived from the risk management process is adequately reported and used as a basis for decision making and accountability at all relevant levels.

Figure 1 describes the necessary components of the framework for managing risk and the way in which they interrelate in an iterative manner.

Figure 1 – Risk Management Framework



Mandate and Commitment

Design of framework for managing risk

- Understanding of the Company and its context (Corporate Plan)
- Establishing a Risk Management Policy (Board Policy)
- Accountability (RACI Matrix)
- Integration into Company processes (Risk Management Strategic Plan)
- Resources
- Establishing internal communication and reporting mechanisms (Risk Management procedure, tools & training)
- Establishing external communication and reporting mechanisms (Risk Management procedure, tools & training)

Continual improvement of the framework
(Risk Management Strategic Plan)

Implementing risk management

- Implementing the framework for managing risk (Corporate Risk Management Plan)
- Implementing risk management processes (Risk Management procedure, tools & training)

Monitoring and review of the framework

Based on: ISO 31000:2009

The Framework applies the Bow-Tie risk assessment methodology that centres on the identification of preventative and mitigation controls in the management of identified potential hazardous events. The objective is always to eliminate risk, however if it is not reasonably practicable to eliminate a risk, then it should be minimised to as low as reasonably practicable (in accordance with the hierarchy of controls). That is elimination followed by substitution, isolation, engineering controls, administrative controls and finally use of personal protective equipment.

The Bow-Tie methodology focuses on assessing the consequence and likelihood of hazardous events affecting each Network company's operations and their ability to deliver specific priority actions and/or programs. Additionally, the Framework incorporates elements from NSW Treasury's recently published "Risk Management Toolkit for NSW Public Sector Agencies" and the NSW Auditor-General's Governance Lighthouse Model.

5.2 Implementing the Risk Management Framework

The framework is not intended to prescribe a management system, but rather to assist the organisation to integrate risk management into the overall management system.

Risk is defined as "the effect of uncertainty on our objectives" and our objectives are detailed in the seven longer term strategic plans relating to health, safety & environment; asset management; finance; risk management; customers; human resources; and technology.

As such, risk management is closely integrated into the business planning cycle. The strategic plans outline the desired outcomes in key areas of business operations and the challenges to be faced in delivering these outcomes, including the underlying assumptions and risks inherent within the plans.

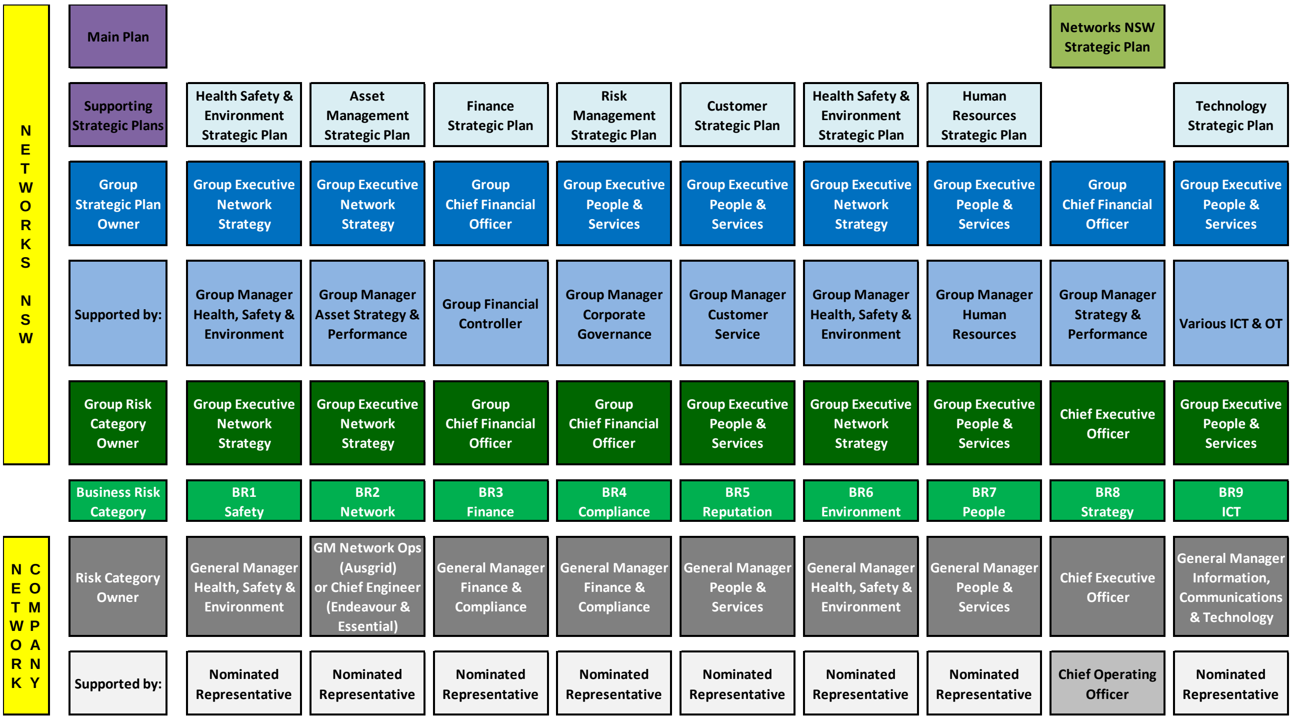
Our annual strategic and operational corporate risk assessment process should, where possible, be timed to coincide with business plan development in order that the required treatment actions are adequately resourced.

These linkages are further strengthened through the use of nine business risk categories (see **Table 1**) and linking both Group and company level responsibilities as well as strategic plans to each category as detailed in **Figure 2** below. Systemic weaknesses in the risk framework identified by Risk Category Owners are addressed in the related Strategic Plan.

Table 1 – Business Risk Categories

BR Number	Risk Category	Generic Risk Description	Risk Category Owner
BR 1	Safety	Fatality/serious injury of employee or member of public	General Manager Health, Safety & Environment
BR 2	Network	Significant customer impact related to the Network	Chief Engineer
BR 3	Finance	Significant unbudgeted financial loss	General Manager Finance & Compliance
BR 4	Compliance	Liability associated with a dispute or material breach of legislation, licence	General Manager Finance & Compliance
BR 5	Reputation	Sustained public criticism of Essential Energy	General Manager People & Services
BR 6	Environment	Significant environmental incident	General Manager Health, Safety & Environment
BR 7	People	Failure to deliver performance through people	General Manager People & Services
BR 8	Strategy	Strategic objectives are not delivered and business opportunities are lost	Chief Executive Officer
BR 9	ICT	Significant ICT & OT system failure	General Manager Information, Communications & Technology

Figure 2 – Relationship between the Strategic Plans and the Business Risk Categories



NETWORKS NSW	Main Plan								Networks NSW Strategic Plan	
	Supporting Strategic Plans	Health Safety & Environment Strategic Plan	Asset Management Strategic Plan	Finance Strategic Plan	Risk Management Strategic Plan	Customer Strategic Plan	Health Safety & Environment Strategic Plan	Human Resources Strategic Plan		Technology Strategic Plan
	Group Strategic Plan Owner	Group Executive Network Strategy	Group Executive Network Strategy	Group Chief Financial Officer	Group Executive People & Services	Group Executive People & Services	Group Executive Network Strategy	Group Executive People & Services	Group Chief Financial Officer	Group Executive People & Services
	Supported by:	Group Manager Health, Safety & Environment	Group Manager Asset Strategy & Performance	Group Financial Controller	Group Manager Corporate Governance	Group Manager Customer Service	Group Manager Health, Safety & Environment	Group Manager Human Resources	Group Manager Strategy & Performance	Various ICT & OT
	Group Risk Category Owner	Group Executive Network Strategy	Group Executive Network Strategy	Group Chief Financial Officer	Group Chief Financial Officer	Group Executive People & Services	Group Executive Network Strategy	Group Executive People & Services	Chief Executive Officer	Group Executive People & Services
	Business Risk Category	BR1 Safety	BR2 Network	BR3 Finance	BR4 Compliance	BR5 Reputation	BR6 Environment	BR7 People	BR8 Strategy	BR9 ICT
NETWORK COMPANY	Risk Category Owner	General Manager Health, Safety & Environment	GM Network Ops (Ausgrid) or Chief Engineer (Endeavour & Essential)	General Manager Finance & Compliance	General Manager Finance & Compliance	General Manager People & Services	General Manager Health, Safety & Environment	General Manager People & Services	Chief Executive Officer	General Manager Information, Communications & Technology
	Supported by:	Nominated Representative	Nominated Representative	Nominated Representative	Nominated Representative	Nominated Representative	Nominated Representative	Nominated Representative	Chief Operating Officer	Nominated Representative

Together with elements of the business planning process, the following documents provide the elements required to implement the framework into the company. They are:

- Risk Management Policy incorporating the common Risk Matrix;
- Risk Management Strategic Plan;
- Corporate Risk Management Plan;
- Risk Management Procedure (including reporting requirements); and
- Risk Management tools and training.

5.2.1 Mandate and commitment

The Board approved Risk Management Policy provides the mandate to implement risk management into the company.

The policy is based on the eleven principles of effective risk management which are taken from ISO 31000:2009 – Risk Management – Principles and Guidelines. These principles state that risk management:

1. creates and protects value;
2. is an integral part of all organisational processes;
3. is part of decision making;
4. explicitly addresses uncertainty;
5. is systematic, structured and timely;
6. is based on the best available information;
7. is tailored;
8. takes human and cultural factors into account;
9. is transparent and inclusive;
10. is dynamic, iterative and responsive to change; and
11. facilitates continual improvement of the organisation.

Implementing the Risk Management Framework and its ongoing effectiveness requires strong and sustained commitment.

Section 7.0 and Annexure A - Risk Management RACI Matrix of this procedure outline the authorities and responsibilities of the Chief Executive Officer, the Chief Operating Officer and the Executive Leadership Team that are required to provide strong and effective leadership of risk management across the company.

5.2.2 Design of the framework for managing risk

The necessary design elements are contained within a series of related company processes as follows:

- understanding of the company and its context is provided through the Strategic Planning process;

- the Risk Management Policy is established by the Board;

- accountabilities have been assigned at a company and Group level as per the policy and procedure, and through the strategic planning process the necessary resources have been allocated; and

- finally, this procedure provides guidance on how to integrate risk management into company processes and outlines the communication and reporting requirements.

5.2.3 Implementing risk management

The Risk Management Board Policy will be utilised by employees to support the promotion of a positive risk culture based on the company's commitment to the management of risk. It contains the common Risk Matrix that reflects the risk appetite approved by the Board. As such, the risk ratings derived using this matrix should be used wherever possible when assessing risks that may have a significant impact on the company.

This procedure is not intended to replace established risk-based processes used to assess site or task specific health and safety or environment risks.

Not all aspects of the common risk assessment process are utilised when undertaking a risk assessment. Guidance on where the company will implement elements of the risk assessment process described in Section 5.3 includes but is not limited to that summarised in Table 2.

Table 2 – Requirements to use elements of the common risk assessment procedure

Risk Assessment for:	Common Risk Matrix ratings	Risk consequence and likelihood criteria	Develop Bow-Tie diagram
Corporate Risk Management Plan	Yes	Common	Yes
Fraud Risk Register	Yes	Common	No
Major business changes	Yes	Common	No
Major capital projects	Yes	Modified	Yes
Major IT projects	Yes	Modified	No
Asset management investment prioritisation	Yes	Modified	No
Business Continuity – Business Impact Assessment	Yes	Modified	No
Litigation Risk Assessment	Yes	Modified	No

Modified consequence and likelihood criteria for projects can be found in Section 5.3.4, other criteria, approved for use by the Risk Manager should be detailed in relevant procedures or workplace instructions.

Risk management will be embedded into the company's practices and processes, particularly into policy development, strategic planning, change management and project management processes. At the corporate level, the Risk Management Framework and risk management process will be applied to the development of a Corporate Risk Management Plan.

Risks identified as having a significant impact on the company's objectives are detailed within the Corporate Risk Management Plan and are categorised as follows:

- Strategic Risks – linked to development and delivery of the Group Strategy;
- Network Fatal Risks – associated with identified potentially fatal work activities; and
- Operational Risks – linked to day-to-day operations.

Developing and maintaining the Corporate Risk Management Plan will be a continuous process, as will the process of managing risk. Newly identified risks and emerging risks that arise as a result of a change in the business environment or through fresh brainstorming, will be incorporated into the Corporate Risk Management Plan. The company will view the Corporate Risk Management Plan as a dynamic, live document.

Prior to the annual refresh of the Corporate Risk Management Plan, the description and naming conventions for the Network Fatal Risks must be confirmed with the Group Manager Health, Safety & Environment.
More generally, risk registers and where required, their associated risk management plans, can be set up for recording the details of risk assessments of specific hazardous events such as other safety risks, project risks or fraud risks.

Risk management plans should be developed in instances where there is a need to monitor ongoing risk. Risk assessments undertaken to support decision making may not require the development of risk management plans.

5.2.4 Training in application of the framework

As a minimum, the Risk Manager will provide either risk awareness training or more detailed technical training in the application of this procedure. Training sessions will be scheduled ahead of the annual Corporate Risk Management Plan refresh and dates published in an annual training calendar. The application of this procedure will be supported by more detailed instructions that can be found in the CEOM0002.24 - Risk Assessment Training Manual.

5.2.5 Monitoring and review of the framework

An effective Risk Management Framework, process and tools that continue to support the company, will require the performance of risk management across the company to be monitored and reviewed. Developments in risk management in the community, including better practices applied in other organisations will be monitored and assessed. The results of the monitoring and review process, together with input from the Network companies, will be captured in the Group Risk Management Strategic Plan and used to update the Risk Management Framework.

5.2.6 Continual improvement of the framework

A Risk Management Strategic Plan will be developed on a three year cycle, with a review annually to identify initiatives to improve the Risk Management Framework.

The Risk Management Strategic Plan will focus on the implementation of the Risk Management Policy, principles contained within the policy, and the integration of effective risk management into the company's key processes.

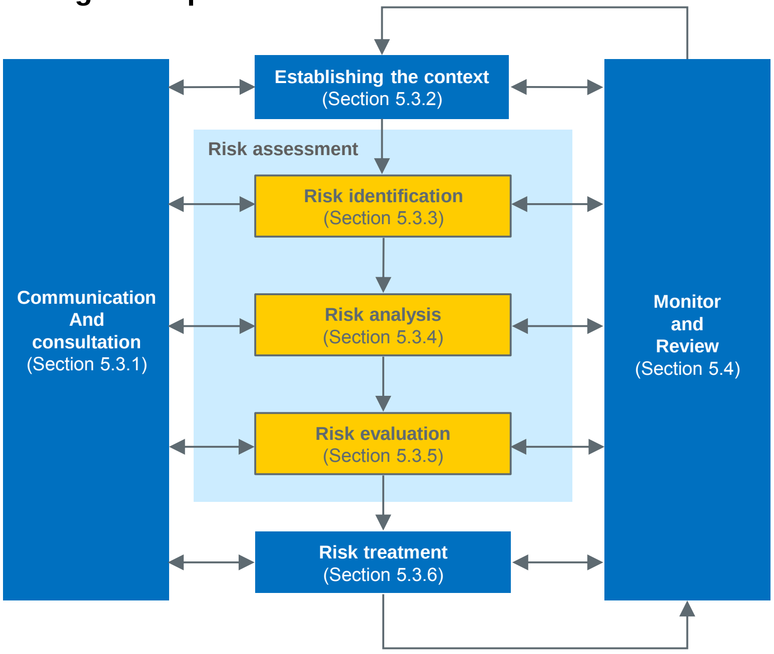
5.3 Risk management process

All managers and employees of the company are responsible for managing risk. A risk is defined as the effect of uncertainty on objectives.

To manage risk, managers and employees will, where required, apply the risk management process defined in this procedure, to identify, analyse and evaluate the effect of uncertainties on their business objectives.

The company's process for the management of risk is based on ISO 31000:2009 and is reproduced in **Figure 3.** Request for support or training in the application of this procedure should be directed to the Risk Manager.

Figure 3 – Risk management process



Based on: ISO 31000:2009

The risk management process should be applied as previously detailed in Section 5.2.3. It is recommended that this risk management process also be applied when there is a requirement to formally document the risks associated with one-off situations.

5.3.1 Communication and consultation

The first step of the risk management process is communication and consultation. Communication and consultation will be undertaken with internal and external stakeholders as appropriate and will be maintained throughout the risk management process (as indicated in **Figure 3**). Employees and managers should plan the communication and consultation process to gain support and input from their colleagues during the earliest stages of the risk management process. It should be noted that the degree of consultation is at the discretion of the person undertaking the risk assessment.
The communication and consultation process should address information and issues relating to the identified risk, its causes, consequences the existing controls and potential alternative controls.

Effective communication and consultation may involve discussions with experienced and knowledgeable persons, literature reviews including the review of previous risk assessments, incident investigations, audit reports, discussion and survey with stakeholders and the community. In an effective, mature risk assessment, consultation and communication will continue throughout the risk assessment process by bringing together employees with differing areas of expertise. This is typically achieved by identifying multi-disciplinary teams of employees in the form of a risk assessment workshop. The consultation process is also important when evaluating risk and for gaining agreement and endorsement for Treatment Action Plans (refer to Section 5.3.6).

Communication and consultation with stakeholders is important as stakeholders make judgements on risk based on their individual perception. These perceptions can vary due to differences in their risk tolerance, needs, assumptions and concerns; however it is important that these differences are explored and taken into account during the risk assessment.

In relation to the annual refresh of the Corporate Risk Management Plan, the Risk Owner must confirm/nominate the subject matter expert for the hazardous event prior to commencement of the assessment. The subject matter expert should lead the technical input to the risk assessment and in consultation with the Risk Manager, should then propose those that are to be consulted during the assessment of the hazardous event.

5.3.2 Establishing the context

The context (internal and external) will be established at the commencement of the risk assessment process, describing the objectives and scope of the risk assessment, and the internal and external parameters to be taken into account when managing the risk. Key elements of the context will be the company's values, purpose, plans and priorities.

Establishment of the context will also include the definition of the risk tolerance for the evaluation of risk. The company's risk tolerance is summarised in **Table 3**.

Table 3 – Risk tolerance

Risk Tolerance
A risk is tolerable when the risk is reduced to as low as reasonably practicable (ALARP).
Risks are also tolerable if they are Non-ALARP and have a Treatment Action Plan in place to reduce the risk to ALARP.
Risks that are Non-ALARP, with no Treatment Action Plan in place are considered intolerable.

Further guidance on determining risk tolerance is presented in section 5.3.5.

5.3.3 Risk identification

Risk identification involves the process of systematically identifying the uncertainties to the achievement of objectives. The uncertainty is expressed in the form of a hazardous event, ie what is the event that will prevent the achievement of the objective? The hazard being any source of harm. It is also important to identify the risks associated with not pursuing an opportunity.
Where specified in **Table 2** or whenever deemed useful, the control environment associated with each risk or hazardous event should be defined in the form of a Bow-Tie diagram.

An example Bow-Tie is shown in **Figure 4**, clearly defining the links between the hazardous event, causes, consequences and controls. Controls will be defined as either preventative controls or mitigation controls. Bow-Tie diagrams will be developed/reviewed and updated in consultation with the Risk Manager to maintain integrity of the data and to manage version control.

The development of a Bow-Tie starts with the identification of uncertainty, hazards or a potential source of harm that will impact an objective. The uncertainty or hazard will then be characterised in the form of a hazardous event and placed at the centre of the Bow-Tie. The causes of the hazardous event will be identified and placed to the left, followed by the consequences on the right.

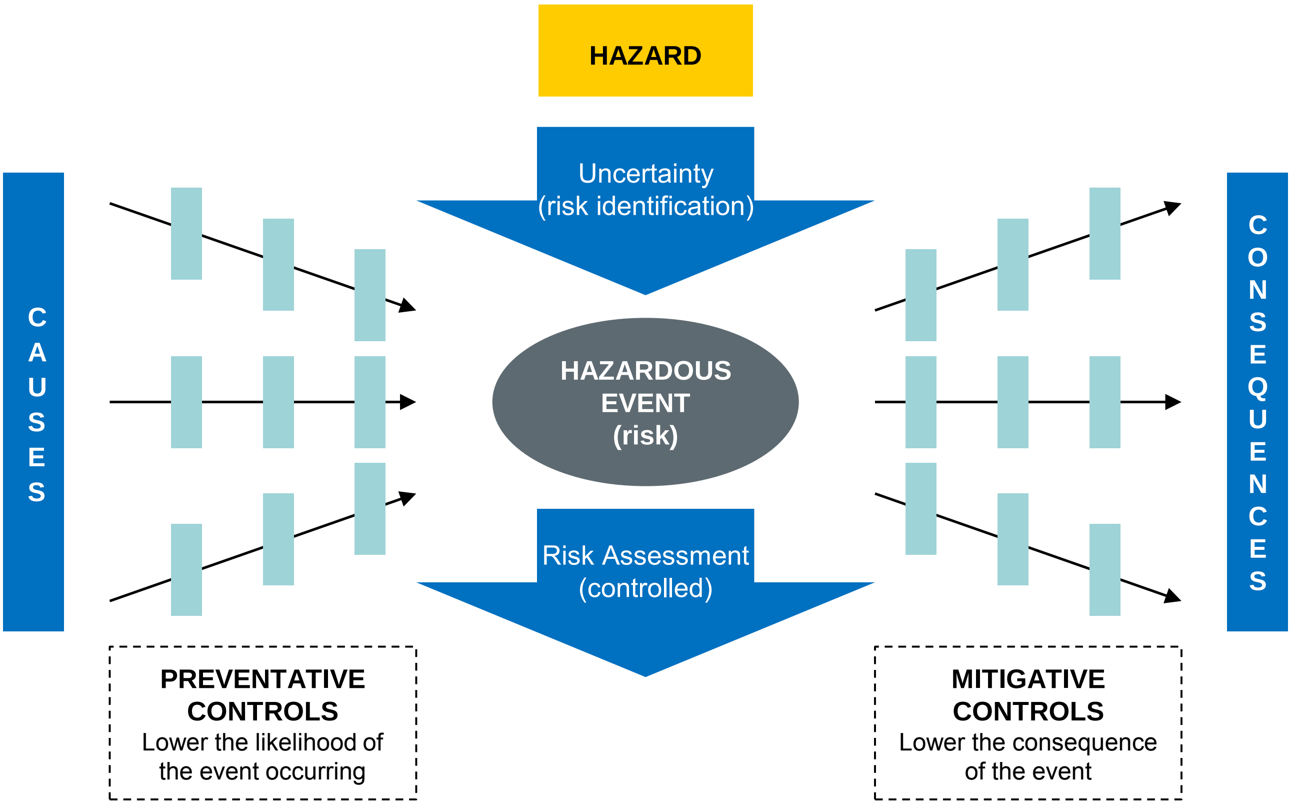
Pathways connecting the individual causes and consequences to the hazardous event will then be drawn, with the primary preventative and mitigation controls placed along each of the pathways, respectively. Primary control weakening factors may also be added to these primary controls to describe mechanisms that may reduce or defeat a primary control's effectiveness. Supporting controls may then be added to show how a control weakening may be detected or prevented.

If the failure of an individual control would result in a significantly weakened control environment, it will be highlighted as a key control.

The results of the Bow-Tie control environment assessment will be reflected in Company Form – Risk Assessment Template and any relevant Bow-Tie diagrams.

For consistency, the Risk Manager will centrally maintain the Bow-Tie diagrams used for the Corporate Risk Management Plan. These Bow-Ties will also be made readily available.

Figure 4 – Bow-Tie diagram



When undertaking a change management risk assessment the first step is to identify all the potential hazardous events that may be triggered by the change, consider any existing controls that might be in place and to risk rate these events using the common Risk Matrix. The change management risk assessment will be documented using Company Form – Change Management Risk Assessment Template.

When undertaking an assessment of the risk associated with management being unable to demonstrate it has fulfilled its Workplace Health and Safety (WHS) duties, refer to Network Fatal Risks – WHS Legal Risk Assessment Guideline contained in CEOM0002.24 - Risk Assessment Training Manual.

The final step in the Bow-Tie process is to identify gaps in the control environment and to assess the overall control effectiveness. Refer to **Table 4** for rating details.

Table 4 – Control environment effectiveness ratings

Descriptor	Rating
Nothing more to be done except review and monitor the existing controls, which are well designed for the risk, address the root causes, and are believed to be effective and reliable at all times.	5 – Effective
Controls are in place, well designed and effective. The operating effectiveness of some controls could be improved or there may be some doubts about their effectiveness and reliability.	4 - Satisfactory
While the design of controls maybe largely correct, in that they treat most of the root causes of the risk, they are not currently very effective. Or: Some of the controls do not treat the root causes even if those that are correctly designed are operating effectively	3 – Poor
Significant control gaps. Either controls do not treat root causes or they do not operate effectively.	2 - Very Poor
Virtually no controls in place and those that are in place have very limited operational effectiveness or are poorly designed	1 - None

5.3.4 Risk analysis

An analysis of each identified hazardous event will be undertaken in a consistent manner using the common Risk Matrix as identified in the Risk Management Policy and Company Form – Risk Assessment Template.

Associated with the common Risk Matrix are consequence criteria that can be used to assess the relative impact on the company associated with Safety impacts, Network impacts, Finance impacts, Compliance impacts, Environment impacts and Reputation impacts.

Note that the 5 levels of consequence described within the common risk matrix should not be used to determine the level of response required to an actual incident. Separate incident response criteria should be established as part of the incident management procedure for this purpose.

The consequence and likelihood criteria expressed in the common Risk Matrix will suit almost all longer term situations, however in the case of assessing the risk associated with a project or program of work, the use of the additional criteria set out in **Table 5** should be considered.

The additional criteria should not be used in isolation but should be used in conjunction with assessments of the main criteria contained in the common Risk Matrix.

Table 5 – Additional criteria for projects

Consequence	Description
Severe	Greater than 50% of Program / Project baseline schedule or budget
Major	Greater than 25%, but less than 50% of Program / Project baseline schedule or budget
Moderate	Greater than 10%, but less than 25% of Program / Project baseline schedule or budget
Minor	Greater than 5%, but less than 10% of Program / Project baseline schedule or budget
Insignificant	Less than 5% of Program / Project baseline schedule or budget
Likelihood	**Description**
Almost Certain	The event has occurred more than once on the majority of similar Projects in the past
Likely	The event has occurred in the majority of similar Projects in the past
Possible	The event has occurred in the minority of similar Projects in the past
Unlikely	The event is known to have occurred on similar projects in the past but only rarely
Rare	The event has not occurred in similar Projects in the past but could

The risk analysis will consider three measures:

1. Inherent risk;
2. Control environment effectiveness; and
3. Residual risk rating.

The inherent risk rating is based on the plausible worst case scenario assuming the absence of company established controls but with the presence of existing external controls such as regulations, road rules etc. and reliance on common sense.

The residual risk is defined as the risk rating based on the plausible worst case scenario with the existing controls in place and operating with the identified control environment effectiveness as at the time of the assessment.

Details of the control environment effectiveness ratings, the inherent risk rationale and risk rating, the residual risk rationale and risk rating will be documented in Company Form – Risk Assessment Template or Company Form – Change Management Risk Assessment Template.

5.3.5 Risk evaluation

Each hazardous event will be evaluated against the company's risk appetite and risk tolerance to determine which risks are tolerable based on their existing controls, and which risks require treatment and the development of Treatment Action Plans. As detailed in Section 5.3.2, a risk is deemed tolerable if it is considered to be:

- "As Low As Reasonably Practicable" (ALARP); or
- Non-ALARP with treatment action plans in place to move the risk to ALARP.

Table 6 provides guidance for evaluating the risk in order to determine its ALARP status.

Table 6 – ALARP status test

Effectiveness of control design	
Do the controls meet regulatory or other mandatory standards? eg have they been applied in accordance with the hierarchy of controls.	**Yes/No**
Has the nature of the risk changed since controls were implemented, and if so, do the controls still manage the risk effectively?	**Yes/No**
Are the controls comparable to peers or accepted industry practice?	**Yes/No**
Operating Effectiveness	
Do the results of monitoring activities tell us our controls are operating effectively, eg are they fit for purpose, suitable for the nature/duration of the work and correctly installed, set up and used?	**Yes/No**
Have recommendations from recent audits in relation to the controls been implemented?	**Yes/No**
In recent incident / near miss events, did the controls work as intended?	**Yes/No**

Below are matters which must be considered when evaluating a health and safety duty:

Has the company considered bringing in other parties with the relevant skills and expertise to advise on the implementation of additional controls to either eliminate, or where not reasonably practicable to eliminate, to then minimise the risk to as low as reasonably practicable?	**Yes/No**
A "**Yes**" response to the above question and those in Table 6 may indicate that existing controls are working well and no new or revised controls are required and therefore the risk is ALARP. If the response to any of the above questions was "**No**", then ways exist to eliminate the risk, or where not reasonably practicable to eliminate, to then minimise the risk to as low as reasonably practicable.	
Are the cost, effort and resources required to eliminate the risk or where not reasonably practicable to eliminate the risk, to then minimise the risk to as low as reasonably practicable, grossly disproportionate to the likely reduction in either consequence and/or likelihood associated with the hazardous event?	**Yes/No**
A "**Yes**" response to the above question may indicate that: • it is not reasonably practicable to implement additional controls to either eliminate the risk, or where not reasonably practicable to eliminate the risk, to then minimise the risk to as low as reasonably practicable; and • the hazardous event may have ALARP status. A "**No**" response to the above question may indicate that: • new controls are reasonably practicable to implement; and/or • existing controls require strengthening; and • the hazardous event may have Non-ALARP status.	

Guidance in determining what is reasonably practicable to meet a health and safety duty

Under the s.18 of the *Work Health and Safety Act 2011 (NSW)*, the following is stated in relation to what is "reasonably practicable" in ensuring health and safety:

In this Act, ***reasonably practicable***, in relation to a duty to ensure health and safety, means that which is, or was at a particular time, reasonably able to be done in relation to ensuring health and safety, taking into account and weighing up all relevant matters including:

(a) the likelihood of the hazard or the risk concerned occurring, and

(b) the degree of harm that might result from the hazard or the risk, and

(c) what the person concerned knows, or ought reasonably to know, about
  (i) the hazard or the risk, and
  (ii) ways of eliminating or minimising the risk, and

(d) the availability and suitability of ways to eliminate or minimise the risk, and

(e) after assessing the extent of the risk and the available ways of eliminating or minimising the risk, the cost associated with available ways of eliminating or minimising the risk, including whether the cost is grossly disproportionate to the risk.

Further guidance on the above can be found in the following Safe Work Australia publication: *"How to determine what is reasonably practicable to meet a health and safety duty", May 2013.*

The responses to the ALARP status test questions must be recorded on the relevant risk assessment spreadsheet.

After considering the ALARP status in your workshop/meeting, the risk rating and ALARP status are to be validated with the relevant Risk Owner or Project/Program Sponsor prior to initiating any treatment actions.

To test the rationale of their evaluation Risk Owners or Project/Program Sponsor are encouraged to ask "would our stakeholders be surprised if we announced a loss due to this risk?" Where the answer is "yes", the effectiveness of the existing control environment, along with the options to further reduce the risk should be investigated further.

5.3.6 Risk treatment

When the results of the risk evaluation determine a risk to be Non-ALARP, risk treatment options will be identified and a Treatment Action Plan documented. Risk treatment involves selecting one or more options for modifying risks, and implementing those options. Once implemented, the treatment action provides additional controls or modifies/improves existing controls. Any business as usual activity undertaken to reduce risk is considered an existing control and is not to be included as a treatment action in a risk management plan. Implementation of a treatment action should result in a significantly improved control environment.

Options for risk treatment include:

- avoiding the risk by deciding not to commence the activity associated with the risk;
- removing the source of the risk;
- changing the likelihood;
- changing the consequence;
- sharing the risk with another party eg insurance, contracts and risk financing; and
- retaining the risk by informed decision (hence revising the risk evaluation).

Once a risk treatment option has been identified, it may be necessary to revisit the risk evaluation in order to determine if it is reasonably practicable to implement. The process of determining if a risk treatment option is reasonably practicable may involve some form of cost-benefit analysis which should be developed on a case by case basis.

All Treatment Action Plans will include a responsible manager and due date for implementation. Treatment actions do not necessarily need to have a completion date within the life of the current risk management plan, in many instances, the due date will be in a subsequent year and the treatment action will carry over in the following year's risk management plan.

The Risk Owner or Project/Program Sponsor is required to endorse any treatment actions and in doing so confirms that the necessary resources will be made available to complete the actions within the designated timeframes.

5.4 Monitor and review risk management

The monitor and review phase must be embedded as part of the risk management process, eg it may be necessary to revise controls in the following circumstances:

- where the risk is non- ALARP;
- where a new hazardous event is identified;
- before a change is implemented; or
- where a need is identified following consultation.

Key Risk Indicators will be established for all risks contained in a risk management plan. Where Key Risk Indicator performance declines, corrective actions to restore control should be developed and implemented.

The implementation of Treatment Action Plans provides a risk management performance measure.

Risk Category Owners and/or Project/Program Sponsors are responsible for reviewing and monitoring the implementation of Treatment Action Plans and the status of Key Risk Indicators. In certain circumstances, a change control process may be required for Treatment Action Plans eg implementation date. The process for facilitating this change is outlined in Company Procedure – Changes to Risk Based Management Plans.

The Manager Governance, Risk & Compliance will establish the monitoring and reporting process for all aspects of the Corporate Risk Management Plan, which includes:

- monitoring that controls are in place, maintained and remain effective;
- identifying further options for risk treatment to reduce the risk further;
- monitoring the implementation of Treatment Action Plans on a monthly basis;
- analysing and learning from events and near misses, including the performance of controls;
- monitoring trends in Key Risk Indicator performance;
- detecting changes in the context, both external and internal; and
- identifying emerging risks.

The annual update of the Corporate Risk Management Plan is one of the major review activities undertaken during the year. Assurance over this process is provided as follows:

- Risk Category Owner endorsement of risk ratings, ALARP status, risk treatment actions and key risk indicators for the hazardous events in their Risk Category;
- review and endorsement of the draft Corporate Risk Management Plan by the Executive Leadership Team;
- review of the draft Corporate Risk Management Plans for the three Network companies by the Group Risk Category Owners; and
- review and endorsement of the draft risk profiles by the Executive Leadership Group prior to provision of the Group risk profile to the Audit and Risk Committee for their information.

The Corporate Risk Management Plan is a dynamic document and there may be a need to re-assess particular hazardous events throughout the year in the following circumstances:

- deteriorating key risk indicator trend;
- emerging risk realisation;
- major organisational change;
- major changes in internal/external context; or
- significant changes to legislation.

At the completion of all treatment actions, the ALARP status does not automatically revert to ALARP. A full re-assessment is required to be undertaken to confirm that the hazardous event has moved from Non-ALARP to ALARP. This re-assessment would typically be undertaken as part of the annual update of the Corporate Risk Management Plan. Should the re-assessment be undertaken ahead of the annual update, and this results in a change of risk rating or ALARP status, the existing Corporate Risk Management Plan can be updated following Company Procedure – Changes to Risk Based Management Plans.

5.5 Risk reporting

Risk management performance will be measured, monitored and reported using the following metrics:

- Treatment Action Plan Implementation Status.
- Key Risk Indicator Trend.

Monitoring and reporting of performance on the implementation and effectiveness of controls associated with the Corporate Risk Management Plan will be provided for noting at the respective meetings of the Executive Audit Risk & Compliance Committee (EARCC). A summary report focused on the Strategic Risks, Network Fatal Risks and “High” Non-ALARP Operational Risks will be presented to the Board and the Audit & Risk Committee (ARC).

Risk Category Owners are to provide an update to the EARCC on the status of hazardous events in their Risk Category as per the timetable set by the Risk Manager and endorsed by the EARCC.

In some cases, treatment actions plans may be carried over to the following financial year, which may result in “orphan” treatment actions plans that do not align to a hazardous event as the hazardous events may have been removed. The “orphan” treatment action plans will be reported as carry over items as part of the update provided to the EARCC. If the “orphan” treatment action plan is related to prior a Strategic Risk, Network Fatal Risk or “High” Non-ALARP Operational Risk, it will be reported as part of the summary report presented to the ARC.

Where applicable, risk reports should also be provided to respective governance committees eg Executive Health, Safety and Environment Committee, Project Steering Committees in line with company reporting processes.

Templates for risk reporting are produced by the Governance, Risk & Compliance Branch.

In addition to the above, the identification and analysis of emerging risks will be conducted in conjunction with the company’s strategic planning process.

5.6 Emerging risk reporting

5.6.1 Emerging risk identification

The identification of emerging risk is a continuous process. The company will employ a range of techniques to identify or sense emerging risks with some examples presented in **Table 7**. The need to facilitate a specific emerging risk identification workshop will be at the discretion of the General Manager Finance & Compliance. Otherwise emerging risks should be brought to the attention of the Risk Manager through the sources identified in **Table 7**.

Table 7 – Emerging risk identification sources

Technique	Description
Risk Assessment	Emerging risk identification workshops. Formal risk identification sessions designed to brainstorm uncertainties in the delivery of strategy and the dependability of the underlying business value drivers. This can involve scenario analysis and stress testing of underlying assumptions.
Employee leads	From employees in risk management, eg Divisional GRC representatives, internal audit or strategic planning. May also be identified at Executive and/or Board planning days.
External sources	External consultants and agencies. The assignment of external experts to conduct consultancy activities that provides information on trends, company performance, contextual developments.
Issues survey	A survey of the company employees designed to identify issues that may impact the operation, strategic execution or reputation of the company.

Fundamental to a robust process of emerging risk identification is:

- the risk identification process must challenge the validity and dependability of the core underlying assumptions and business value drivers detailed in the Strategic Plans;
- the ability to draw a relationship between the uncertainty and the Priority Actions of the company, in order to test that the uncertainty is not simply a distraction; and
- the process allows for consideration of unexpected, low-probability events with the potential to have a high-impact on the company.

5.6.2 Risk analysis

Due to their nature, many emerging risks material to the company are high-impact, low probability. As a result, the analysis of an emerging risk will not focus so much on the likelihood of the risk, but on the *speed of onset* of the risk; that is: how quickly (in terms of time) the impact of the risk will be felt by the company.

Speed of onset is an expression of time (as opposed to probability) and is expressed in terms of months.

The analysis of emerging risk will be undertaken on two parameters:

- plausible worst case consequence; and
- speed of onset (velocity).

Table 8 provides a sample of *speed of onset* durations which can be used in the communication of emerging risks.

Table 8 – Speed of onset durations

Speed of Onset	Time
Very rapid	Less than 3 months
Rapid	Greater than 3 months, but less than 12 months
Slow	Greater than 12 months

The consequence will be assessed using the criteria assigned to the company's common Risk Matrix as defined in Board Policy – Risk Management.

The analysis of consequence should be supported with a qualitative statement on the magnitude of the impact. This is important, because in some circumstances the magnitude may well exceed the definition of "Severe" contained on the company common Risk Matrix. In addition, it is good practice to include a narrative of the impact in risk reporting.

5.6.3 Emerging risk response

The response to an emerging risk can be one of four actions outlined in **Figure 5** below:

Figure 5 – Matrix for response to emerging risk

	Velocity		
Consequence	Slow	Rapid	Very Rapid
Severe	Prepare for	Act upon	Act upon
Major	Prepare for	Prepare for	Act upon
Moderate	Park	Adapt to	Adapt to
Minor	Park	Park	Adapt to

Emerging Risk Response

Act upon	Severe/major consequence, high velocity risks are acted upon. Action is taken to directly respond to the risk - strategy &/or plans changed.
Prepare for	Severe/Major consequence low velocity risks - plans are put in place to prepare the business to manage the risk.
Adapt to	Moderate/minor consequence, high velocity risks are adapted too.
Park	Moderate/minor impact, low velocity risks are parked. Not material in impact and travelling with low velocity hence no need to adapt strategy or plans.

If uncomfortable:……
- Do we know enough?
- Is the impact underestimated?
- Could the risk move faster than estimated?

The initial assessment must be validated with the relevant Risk Category Owner before being documented in Company Form – Emerging Risk Register. Where emerging risks with severe or major consequences have been identified, a risk assessment should be undertaken in line with this procedure and Treatment Action Plans developed.

Any Treatment Action Plans should be validated against the *speed of onset* to confirm that the control can be implemented ahead of the expected onset.

5.6.4 Emerging risk reporting

Emerging risks will be reported alongside known risks in the Risk Management Report. When an emerging risk is identified it will be assigned to a risk category.

Emerging risks will be detailed in the Risk Management Report to the EARCC. In preparing the report, the Risk Manager should consider all identification methods. Typically this will involve interviews with Risk Category Owners, or their representatives, focusing on issues identified in recent surveys and any other matters that have the potential to impact delivery of Priority Actions.

6.0 RECORDKEEPING

The table below identifies the types of records relating to the process, their storage location and retention period.

Type of Record	Storage Location	Retention Period*
Risk Management Strategic Plan	Essential recordkeeping system	Required as State Archives – as per GA28 section 19.14.01
Corporate Risk Management Plan	Essential recordkeeping system	Destroy 6 years after date closed – as per GA28 section 19.19.01
Approved change requests to the Corporate Risk Management Plan	Essential recordkeeping system	Destroy 6 years after date closed – as per GA28 section 19.19.01
Final version of bowties	Essential recordkeeping system	Destroy 6 years after date closed – as per GA28 section 19.19.01
Final version of Risk Assessment spreadsheets	Essential recordkeeping system	Destroy 6 years after date closed – as per GA28 section 19.19.01
Risk Management reports submitted to the EARCC	Essential recordkeeping system	Required as State Archives – as per GA28 section 19.17.02
Risk Management reports submitted to the ARC	Essential recordkeeping system	Required as State Archives – as per GA28 section 19.17.02
Risk management plan	Essential recordkeeping system	Destroy 6 years after date closed – as per GA28 section 19.19.01
Project risk management plan	Essential recordkeeping system	Destroy 6 years after date closed – as per GA28 section 19.19.01
Change management risk assessment	Essential recordkeeping system	Destroy 6 years after date closed – as per GA28 section 19.19.01

* Content Coordinator must liaise with the Records Manager to validate the retention period is compliant with the relevant disposal authority.

7.0 AUTHORITIES AND RESPONSIBILITIES

Chief Executive Officer has the authority and responsibility for:

- approving this procedure;
- demonstrating leadership and commitment to the implementation of the Risk Management Framework across the company; and
- endorsing the Risk Management Strategic Plan.

Executive Leadership Group and **Executive Leadership Team** have the authority and responsibility for:

- allocating resources to maintain compliance with this procedure;
- demonstrating leadership and commitment to the implementation of the Risk Management Framework across the company;
- endorsing the risk ratings and ALARP status of the hazardous events contained in the company risk profile;
- embedding risk management into the key business processes including, but not limited to policy and procedure development, strategic planning, change management and project management processes;
- reporting changes to the risk profile including emerging risks to the company and the Board in line with the reporting criterion defined in this procedure;
- monitoring and reviewing risk management performance, including treatment action status and key risk indicator trends; and
- developing and implementing additional treatment actions to address any significant decline in risk management performance identified through the monitoring.

Group Executive People & Services has the authority and responsibility for developing and maintaining the Risk Management Framework and the Risk Management Strategic Plan.

Group Manager Corporate Governance has the authority and responsibility for:

- consulting with Network companies to develop the Risk Management Framework;
- facilitating Risk Management Reports to the Audit and Risk Committee; and
- undertaking an independent review of the Risk Management Framework on behalf of the Audit and Risk Committee.

Group Manager Health Safety & Environment has the authority and responsibility for confirming the Network Fatal Risk titles and descriptions for inclusion in the annual refresh of the Corporate Risk Management Plan.

Group Risk Category Owners have the authority and responsibility for:

- undertaking risk assessments to support the delivery of the Strategic Plans using the risk management process contained within this procedure; and
- reviewing and endorsing the risk ratings and ALARP status of the hazardous events included in their risk category as provided by the Network companies.

General Manager Finance & Compliance has the authority and responsibility for establishing appropriate governance mechanisms to support the implementation and ongoing management of the Risk Management Framework.

Manager Governance, Risk & Compliance has the authority and responsibility for:

- providing leadership in the development and promotion of a positive risk culture;
- implementing the principles of the Board Policy – Risk Management into the design of the Risk Management Framework;
- implementing the Risk Management Strategic Plan;
- developing and maintaining a Corporate Risk Management Plan to support the delivery of the Corporate Plan using the risk management process contained within this procedure;
- implementing an annual review of the Corporate Risk Management Plan;
- delivery of awareness training and mentoring to continue the development of appropriate risk management skills and competencies in the company;
- establishing the systems and tools to facilitate the risk management process and the implementation of the Risk Management Framework; and
- reviewing this procedure so that it remains current and relevant to the company's needs regularly.

Risk Manager has the authority and responsibility for:

- facilitating the implementation of the Risk Management Framework;
- implementing the initiatives contained in the Risk Management Strategic Plan;
- coordinating with the members of the Executive Leadership Team and their delegates for the development of the Corporate Risk Management Plan;
- coordinating with the members of the Executive Leadership Team and their delegates regarding emerging risk;
- developing mechanisms for monitoring and reporting the company's risk management performance;
- coordinating the collation and assessment of risk performance data and providing regular reports to the Executive Leadership Team and Group Manager Corporate Governance for inclusion in the consolidated reporting to the Audit and Risk Committee;
- maintaining a centralised set of Bow-Tie diagrams to support the Corporate Risk Management Plan;
- maintaining the emerging risk register;
- providing direction and advice on the application of this procedure to Risk Category Owners, Risk Category Nominated Lead and Divisional Governance, Risk & Compliance Representatives; and
- facilitating training sessions on the application of the Risk Management process.

Risk Owners have the authority and responsibility for:

- nominating a subject matter expert to lead technical input to each risk assessment undertaken; and
- endorsing the risk ratings and ALARP status of the hazardous events assigned to them.

Risk Category Owners have the authority and responsibility for:

- reviewing and endorsing the risk ratings and ALARP status of the hazardous events included in their risk category; and
- reporting annually to the Executive Audit Risk & Compliance Committee on the status of the risks in their category.

Divisional Governance, Risk & Compliance Representatives and/or **Risk Category Nominated Leads** have the authority and responsibility for:

- providing support to the division for the implementation of the Risk Management Framework and the Risk Management process;
- providing risk performance data to the Risk Manager, in line with the corporate timetable; and
- liaising with the Risk Manager on matters relating to the implementation or deviation from the Risk Management Framework.

Branch Managers have the authority and responsibility for:

- participating in the development of the Corporate Risk Management Plan as subject matter experts, as required;
- familiarising themselves with the hazardous events contained within the Corporate Risk Management Plan;
- implementing Treatment Action Plans (where relevant) and providing data to monitor trends associated with Key Risk Indicators; and
- communicating and consulting with the relevant Executive Leadership Team member in relation to emerging risks.

Project/Program Sponsors have the authority and responsibility for:

- endorsing the project Risk Management Plan;
- reviewing and endorsing the risk ratings, ALARP status and treatment actions for the hazardous events related to their project; and
- approving the project specific processes for the reporting of material project risks.

Project Managers have the authority and responsibility for:

- complying with the requirements of this procedure when undertaking project risk assessments;
- providing risk performance data to the Project/Program Sponsor; and
- liaising with the Risk Manager on matters relating to the implementation or deviation from the Risk Management Framework for project risk assessments.

Employees have the authority and responsibility for complying with the requirements of this procedure when undertaking risk assessments.

8.0 DOCUMENT CONTROL

Content Coordinator :	Manager Governance, Risk & Compliance
Distribution Coordinator :	GRC Process Coordinator

KEY

- R • **RESPONSIBLE**: The person who is assigned to do the work
- A • **ACCOUNTABLE**: The person who makes the final decision and has the ultimate accountability
- C • **CONSULTED**: The person who must be consulted before a decision or action is taken
- I • **INFORMED**: The person who must be informed that a decision or action has been taken

Annexure A - Risk Management RACI Matrix

			BOARD		GROUP						COMPANY									PROJECTS	
			Board	Audit & Risk Committee	Chief Executive Officer	Executive Leadership Group	Group Risk Category Owners	Group Executive People & Services	Group Manager Corporate Governance	Group Manager Health Safety & Environment	Executive Leadership Team	General Manager Finance & Compliance	Manager Governance, Risk & Compliance	Risk Manager	Risk Category Owners	Risk Owners	Risk Category Nominated Lead	Divisional Governance, Risk & Compliance Representatives	Branch Managers	Project/Program Sponsors	Project Managers
Category	Ref	Activity	R A C I	R A C I	R A C I	R A C I	R A C I	R A C I	R A C I	R A C I	R A C I	R A C I	R A C I	R A C I	R A C I	R A C I	R A C I	R A C I	R A C I	R A C I	R A C I
Risk Management Framework																					
Risk Management Framework	6.0	Develop the Risk Management Framework						A	R				C								
	5.2.2	Designing the Risk Management Framework in line with the Risk Management Policy				C I		A	R				C								
	5.2.1	Implementing the Risk Management Framework									C		A	R				C			
	6.0	Establishing appropriate governance mechanisms to support the implementation and ongoing management of the Risk Management Framework						A				R	C								
	5.2.3	Embed risk management into policy development, strategic planning, change management and project management processes.				R					A										
	6.0	Provide support to the division for the implementation of the Risk Management Framework									A						R	R			
	6.0	Undertake independent review of the Risk Management Framework on behalf of the Audit & Risk Committee		I				A	R				C								
	6.0	Provide leadership in the development and promotion of a positive risk culture						A			R		R								
Board Policy	5.2.1	Approve Risk Management Policy providing the mandate to implement risk management into the company	A																		
	5.2.1	Provide strong and effective leadership of risk management across the company			A	R					R		R	R							
Risk Management Strategic Plan	5.2.5	Develop the Risk Management Strategic Plan on a 3 year cycle					C	A	R				C								
	5.2.5	Undertake delivery risk assessment on respective Strategic Plans					R A														
	5.2.5	Endorse the Risk Management Strategic Plan			A																
	6.0	Implementing the Risk Management Strategic Plan											A	R							
	5.2.5	Annual review of Risk Management Strategic Plan						A	R				C								
Risk Management Plans	5.2.3	Develop the Corporate/Project Risk Management Plan				C	C				C		A	R	C	C	C		C	A	R
	5.2.3	Confirm titles and descriptions of Network Fatal Risks								R											
	5.2.3	Maintain the Corporate/Project Risk Management Plan									C		A	R			C	C		A	R
	5.3.3	Centrally maintain the set of Bow-tie diagrams associated with the Corporate Risk Management Plan											A	R				I			
	6.0	Implement an annual review of the Corporate/Project Risk Management Plan									C		A	R	C	C	C	C		A	R
Risk Management Procedure	6.0	Approve the Risk Management Procedure			A																
	6.0	Provide direction and advice on the application of this procedure to Risk Category Owners, Risk Project Managers and Divisional Governance, Risk & Compliance Representatives											A	R							
	6.0	Regular review of the Risk Management Procedure											A	R							
Risk Management tools and training	6.0	Delivery of awareness training and mentoring to continue the development of appropriate risk management skills and competencies in the company											A	R							
	6.0	Establishing the systems and tools to facilitate the risk management process and the implementation of the Risk Management Framework						A					R	R							

KEY

- R • **RESPONSIBLE**: The person who is assigned to do the work
- A • **ACCOUNTABLE**: The person who makes the final decision and has the ultimate accountability
- C • **CONSULTED**: The person who must be consulted before a decision or action is taken
- I • **INFORMED**: The person who must be informed that a decision or action has been taken

Annexure A - Risk Management RACI Matrix

			BOARD								GROUP																								COMPANY																																				PROJECTS							
			Board				Audit & Risk Committee				Chief Executive Officer				Executive Leadership Group				Group Risk Category Owners				Group Executive People & Services				Group Manager Corporate Governance				Group Manager Health Safety & Environment				Executive Leadership Team				General Manager Finance & Compliance				Manager Governance, Risk & Compliance				Risk Manager				Risk Category Owners				Risk Owners				Risk Category Nominated Lead				Divisional Governance, Risk & Compliance Representatives				Branch Managers				Project/Program Sponsors				Project Managers			
Category	Ref	Activity	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I	R	A	C	I
Risk Management Process																																																																																
Communication & Consultation	5.3.1	Develop mechanisms within the respective division/project for the communication and consultation of risk management information, including mechanisms for the ongoing identification and assessment of risk																																	●	●																															●							●				●			
	5.3.1	Provide guidance and mentoring on the application of the Risk Management process to the Company																																										●			●																															
	5.3.1	Nominate a subject matter expert to lead technical input to each risk assessment undertaken																																																					●	●																						
	6.0	Review and endorse the risk ratings and ALARP status of the hazardous events assigned to them as Risk Owners.																																																					●	●																						
	6.0	Review and endorse the risk ratings and ALARP status of the hazardous events included in their risk category/project																	●																																●	●																			●	●						
	6.0	Endorse risk ratings of the hazardous events contained in the company risk profile								●						●																			●																																											
Monitor & review risk management	5.4	Establish the monitoring and reporting process for any Risk Management Plan (e.g Corporate or Project)																																										●			●																										●			●			
	5.4	Develop mechanisms for monitoring and reporting the Company's risk management performance																																										●			●																															
	5.4	Establish Key Risk Indicators for each risk contained in the Corporate Risk Management Plan																																										●					●										●								●											
	5.4	Review and monitor the implementation of Treatment Action Plans and the status of Key Risk Indicators associated with any Risk Management Plan (e.g. Corporate or Project)																																		●											●																											●			●			
Risk reporting	5.5	Monitoring and reporting of performance on the implementation and effectiveness of controls to be provided for noting at the respective meetings of the Executive Audit, Risk & Compliance Committee (EARCC)																																										●			●																●															
	6.0	Facilitate Risk Management Reports to the ARC																						●			●																		●				●																													
Emerging risk identification	5.6.1	Employ a range of techniques to identify or sense emerging risks, e.g. risk assessment, employee leads, external source, issues survey)																																		●	●								●		●																		●													
	5.6.1	Communicate and consult with the relevant ELT member in relation to emerging risks.																																			●							●			●																				●											
Risk analysis (emerging risks)	5.6.2	Analyse the emerging risk based on consequence (using the Company's risk matrix) and the speed of onset																																		●							●				●																															
Company risk response (emerging risks)	5.6.3	Document initial assessment in the Emerging Risk Register																																										●			●																															
	5.6.3	For emerging risks with severe or major consequences, undertake a risk assessment and develop treatment action plans																																		●											●																															