Risk Management Policy & Framework

Risk & Assurance

Document number:	**RM 001-2006**
Issue number:	4
Status:	Final
Author:	Manager, Risk & Compliance
Sponsor:	General Manager, Risk & Assurance
Approver:	Audit & Risk Management Committee
Date of approval:	27/3/2013
Date for review	27/3/2016
File name	Risk Management Policy & Framework Version 4.0.doc

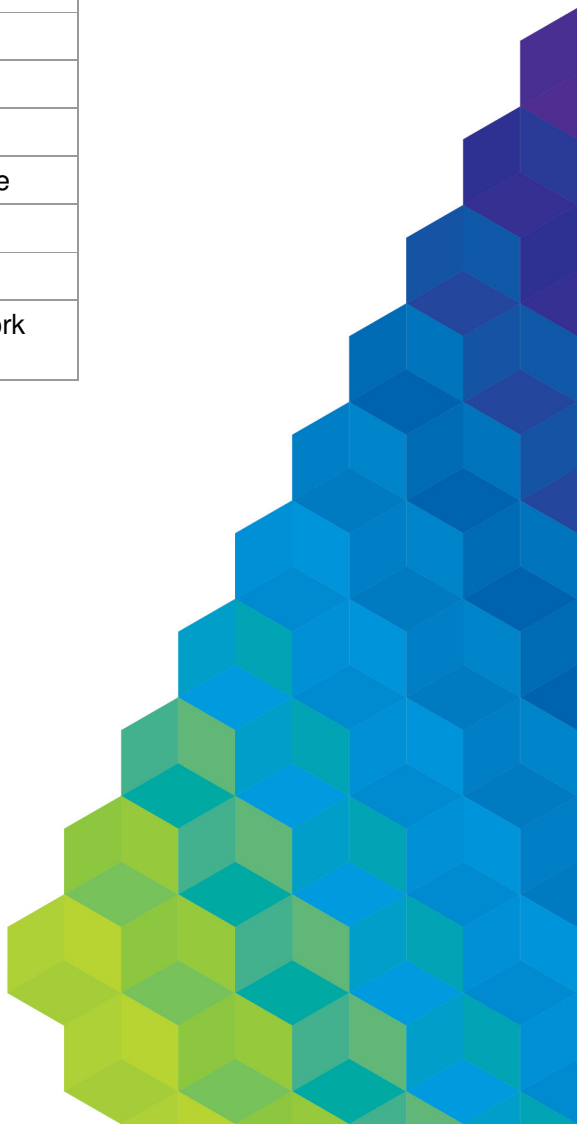


TABLE OF CONTENTS

1 EXECUTIVE SUMMARY

AusNet Services is currently transforming itself to enable it to deal with current and anticipated changes to its market and external environment that pose both threats and opportunities for the company. To enable it to deal with these sources of risk, the Framework will provide a dynamic and responsive support for managers in all forms of decision-making.

The Risk Management Framework design is a document that provides a 'blue print' to managing risk consistently within AusNet Services. The main themes are:

1. Provide simple to use, relevant tools
2. Building capability and motivate effective risk management; and
3. Promote the ownership of risk management by divisions and its integration into the system of management.

The Framework includes:

- A Policy Statement expressing clear mandate and accountability for managing risk;
- An overarching set of Standards that set simple performance requirements for managing risk;
- A comprehensive vocabulary for risk management;
- Each Division of the company incorporating in its annual business planning process a risk management plan that reflects its decisions on the pace and targets for integration – against which its progress will be monitored and reported;
- The use of the Risk Management Information System with appropriate functionality to support the correct behaviours and drive consistency and to allow efficient monitoring and reporting;
- A strategy for training and mentoring all staff, to the required level of competence, so that they can fulfil their responsibilities for managing risk;
- Use of embedded practitioners or 'Coordinators' who will assist practically in the management of risk;
- The Manager, Risk and Compliance and the Risk Management team will lead the changes required and will provide support for other divisions of AusNet Services in the implementation of their risk management plans;
- Using our existing performance management system and leadership accountability standards to drive improvements in the effectiveness of our approach to managing risk; and
- Fostering an active means to share good practice in managing risk and the lessons learned.

Supported by:

- Guidelines, that provide a consistent, generic tool-kit of simple to use methods to satisfy the requirements of the Standards;
- ARMC and GRC oversight of the effectiveness of the Framework; and
- Risk management maturity evaluation model.

2 INTRODUCTION

2.1 Purpose

AusNet Services is required to ensure that there is an effective system of risk management and internal control across the business. It also recognises that focussed and effective risk management creates and protects value, and underpins consistent, reliable performance.

The Risk Management Policy is an overarching statement of the intentions and direction of risk management practice at AusNet Services. The purpose of the Risk Management Framework is to provide the standards and protocols to guide the integration, practice and administration of risk management across the organisations activities to achieve the policy intent.

This framework provides the overarching structure and relationship of the components used to achieve the policy.

The Risk Management Framework is part of AusNet Services' broader governance framework. The Code of Business Conduct takes precedence. Other relevant documents include:

- Board Charter;
- Audit & Risk Management Committee Charter;
- Group Risk Committee Charter;
- Risk Management Policy;
- Fraud Control Policy;
- Whistleblower Policy;
- Authority Manual;
- AusNet Services' Integrated Response and Contingency System (SPIRACS); and
- Leadership Accountability Standards.

2.2 Scope

The AusNet Services' policy is that there will be one, consistent framework for the management of risks across all parts and activities of the company. Risk is defined as uncertainty with the potential to impact on business objectives.

Some of the components of the framework are:

- A Policy Statement expressing clear mandate and accountability for managing risk;
- An overarching set of Standards that set performance requirements for managing risk;
- Supporting guidelines, that provide a consistent, generic tool-kit of simple to use methods to satisfy the requirements of the Standards;
- A practical means for risk analysis and prioritisation;
- A comprehensive vocabulary for risk management;
- Each Division of the company incorporating in its annual business planning process a risk management plan that reflects its decisions on the pace and targets for integration – against which its progress will be monitored and reported;
- The use of the Risk Management Information System with appropriate functionality to support the correct behaviours and drive consistency and to allow efficient monitoring and reporting;
- A strategy for training and mentoring all staff, to the required level of competence, so that they can fulfil their responsibilities for managing risk;
- Use of embedded practitioners or 'Coordinators' who will assist practically in the management of risk;
- The Manager, Risk and Compliance and the Risk Management team will lead the changes required and will provide support for other divisions of AusNet Services in the implementation of their risk management plans;

- Using our existing performance management system and leadership accountability standards to drive improvements in the effectiveness of our approach to managing risk;
- Fostering an active means to share good practice in managing risk and the lessons learned.

2.3 Background

AusNet Services faces uncertainty in achieving its strategic objectives. Those uncertainties arise from its operating environment and the challenges in strengthening, extending, modernising and transforming its internal environment. AusNet Services is currently transforming itself to position it to adapt to current and emerging changes to its market and external environment that pose both threats and opportunities for the company.

The effect this uncertainty has on the company's objectives is 'risk' and to succeed AusNet Services must be proficient in the management of risk – particularly when making decisions and creating changes. Most importantly, when decisions are made to implement business strategies, projects and initiatives, risks must be properly assessed and appropriate responses planned and implemented to ensure the desired outcomes are achieved.

Managing risk is already an integral part of AusNet Services' practices. Risk Management adds structure, discipline and consistency to aligning decisions and priorities to the business objectives, health and sustainability.

Implementing the risk management framework involves:

1. The use of relevant tools to support all forms of decision making;
2. Building capability and motivating effective and consistent risk management; and
3. Promoting the ownership, the principles of transparency and positive assurance in risk management by divisions and its proper integration into all processes for decision-making.

The framework is based on the international standard, ISO 31000 and has been specifically tailored to AusNet Services, its risk profile and the types of decisions, changes and plans that it has to make.

The implementation of the framework should lead to AusNet Services having enhanced resilience and greater agility.

2.4 Risk Management Philosophy

AusNet Services recognises the importance of effective risk management and is committed to improving its risk management processes and capabilities throughout its business. Risk management is about recognising the effects of uncertainty on objectives and making sure the risks are aligned with corporate and divisional objectives. AusNet Services' risk management process enables enhanced decision making, supports effective change management and provides an environment of continuous improvement. The Framework provides a 'blue print' to managing risk in AusNet Services as effective and efficiently as possible.

2.5 Value Proposition

The benefits from adopting and embedding the risk management framework are that:

- Accountability for managing risk is clearly allocated in keeping with all other aspects of management;
- Important decisions are properly informed as to the risks involved and how these can best be treated to ensure a high likelihood of success;
- There will be a high degree of confidence that the company will achieve its objectives;
- There will be a high degree of confidence that projects and initiatives will be successful;

- Overall, losses will be minimised and gains enhanced;
- There will be support for a culture of recognising viable opportunities and acting upon them;
- The control environment for the company will be optimised which may lead to efficiencies and reduce the burden on staff;
- There will be one, consistent system for managing all forms of risk; and
- AusNet Services is able to demonstrate effective Governance to its stakeholders and ensure their confidence.

3 RISK MANAGEMENT FRAMEWORK OUTLINE

3.1 Risk Management Policy Statement

Risk Management Policy Statement

The effective management of risk is central to the **continued growth and success** of AusNet Services. By understanding and managing risk, we can provide **greater certainty** for our securityholders, employees, customers and suppliers and the communities in which we operate. Being better informed, more decisive, we have increased confidence to move to **achieve our purpose** of providing our customers with superior network and energy solutions.

By **understanding and responding to the sources of uncertainty** for our strategic objectives, we ensure our existing business becomes **more resilient** so that we improve service delivery, achieve operational excellence and enhance our ability to deliver on our objectives. Effective risk management will also help us become more agile, to support the development and growth of a modern, diversified portfolio of utility businesses that **provide customers with superior, innovative and sustainable energy solutions**.

Throughout the company we adopt a structured and consistent process for recognising, understanding and responding to risk. **All employees are responsible for the management of risk** in accordance with the company Risk Management Standards. This responsibility includes ensuring that **emerging conditions and key controls are identified** and monitored so that any early warning of failure leads to pre-emptive action.

We operate under **one framework** that enables the management of risk to become fully integrated into all our critical systems and processes for making decisions. This enables us to challenge assumptions and preconceptions before decisions are made and then take appropriate actions to reduce uncertainty that our objectives will be achieved.

All Divisions will be responsible for developing and implementing their plans for this **integration**, based on their strategic and operational needs. Information about risks and how they are to be treated will be documented in the Risk Management Information System and kept up to date through regular review.

We identify and prepare response and recovery plans for potential disruptive events that may seriously threaten our business. After events and incidents occur, we use systematic processes to **learn about our successes and failures**. In this way, we drive continuous improvement in the way we manage risk.

Good corporate governance will be assured through the regular measurement and reporting of our risk management performance to the Group Risk Committee and the Board and Audit and Risk Management Committee.

We will commit the necessary resources to ensure that this policy is satisfied.

Nino Ficca

Managing Director

3.2 Risk Management Standards

Table 1: Risk Management Framework Standards

Standards		Summary requirements
1	Integrating risk management into decision making	Before any significant decision for major projects or initiatives, or when significant internal or external changes are planned or identified, a suitable risk assessment will be conducted to determine the most appropriate course of action. The risk management process will be integrated into all the processes we use to make significant decisions and to deal with changes.
2	Integrating risk management into planning	The risk management process will be integrated into the process for developing all business and strategic plans in order to identify the material risks to the achievement of AusNet Services' objectives.
3	Assuring key controls	Key controls will be identified and allocated to nominated control owners for periodic verification that they are adequate, effective and cannot be cost effectively improved. The effectiveness of key controls will be monitored using lead indicators.
4	Learning from successes and failures	After any significant incident, event, change or decision an analysis will be conducted to learn from both successes and failures. This will include the use of root cause analysis.
5	Analysing risks and controls	Risks will be rated and prioritised for attention using a consistent process of risk analysis. The process will involve estimating Control Effectiveness and using the AusNet Services' risk rating tables to arrive at the current level of risk. Potential Exposure will be used as a measure to focus and plan control assurance activity. Potential Exposure will be estimated for each risk in terms of the total plausible worse case impact arising from a risk assuming all current controls fail.
6	Evaluating risk	Risk evaluation will be undertaken in order to determine if further treatment is required taking into account costs and other disadvantages compared with benefits. The AusNet Services' Risk Matrix will be used to determine the level of risk and priority for attention. Sign off will be required for the continued tolerance of the assessed level of risk as shown. Authority for continued toleration of a level of risk will be required if the risk treatment is not taken within the time suggested.
7	Treating risk	All options for treating risk will be considered and will include: • Avoiding the risk; • Changing the likelihood; • Changing the consequences; • Sharing the risk with another party; and • Tolerating the risk without further treatment. Risk treatment actions will be allocated to people who will be accountable for their completion.

Standards		Summary requirements
8	Accountability for managing risk and resources	The Manager, Risk and Compliance will be responsible for ensuring consistent application of the risk management process across AusNet Services. Each division will appoint at least one risk management coordinator who will lead compliance with these Standards. ELT members will be responsible for maintaining their headline risk registers and ensuring risk management is active and effective in their areas of the company. Risk owners will be nominated for all risks. Risk owners will be accountable for ensuring that appropriate risk treatment occurs and that risks are appropriately rated, monitored and reviewed. Control owners will be nominated for all key controls and will be accountable for verifying that controls are adequate and effective. Task owners will be nominated for all risk treatments and will be accountable for ensuring agreed tasks are completed on time.
9	Planning and recording risk management	Each division will prepare and maintain a risk management plan that will be reviewed at least annually. Each major project will prepare and maintain a risk management plan that describes how risks will be managed in each phase of the project. All risk management information for AusNet Services, divisions and projects will be held in the Risk Management Information System unless agreed otherwise.
10	Governance reporting of risk management	The GRC and the ARMC will receive regular reports on the headline risks, any changes to these and the reasons for changes. The ARMC will oversee the progress made in the implementation of these Standards and on the effectiveness of risk management across the company.

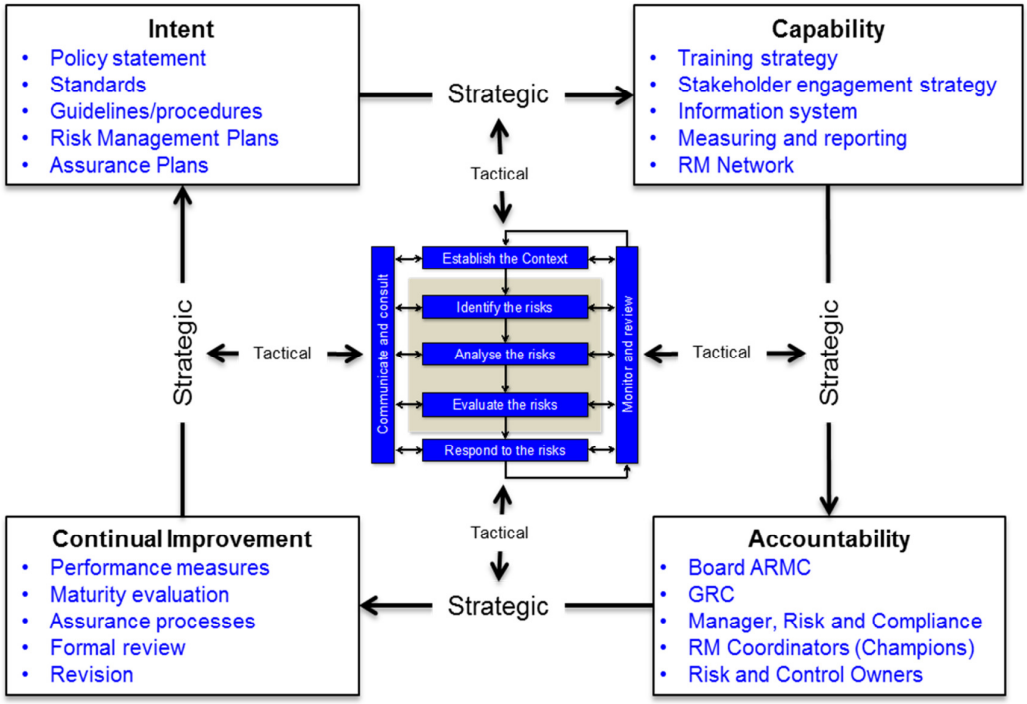
The Standards contain a consistent set of definitions to be used across the company. Standard 5 references the risk rating system to be applied across the company in all its operations and initiatives. Refer to Appendix 1. The consequence criteria aligns with AusNet Services' current objectives and critical success factors. The descriptions for the same level for different consequence types are aligned. Only one system for the qualitative analysis of all risks will be used for the initial analysis and screening of all types of risks.

Standard 6, containing requirements for risk evaluation, specifies the level of the organization where the continued toleration of residual risks at a designated level will be signed off. These requirements drive governance reporting.

The Risk Management team is responsible for the preparation of the guidelines that specify best practice methods which provide managers with simple and relevant tools they can use to manage risk in support of decisions - as an integrated activity.

3.3 Risk Management Framework Outline

Figure 1 shows the general structure of the framework AusNet Services will deploy. It is based on the AS/NZS ISO 31000:2009 standard for risk management.



The figure shows two cycles: the innermost one is the well-known process that is at the core of tactical risk management. Surrounding the tactical process is the strategic envelope representing how AusNet Services will drive and focus risk management according to:

- Stakeholders' needs;
- Business objectives;
- The desired culture;
- Business Model and Organisational Structure;
- The need for control and risk management assurance;
- Governance reporting requirements.

3.4 Intent

The Policy sets the intent and is the means by which the company determines and signals to stakeholders, what it is intending to achieve in its management of risk and establishes a mandate from the Managing Director and provides an externally reviewable statement of commitment. The Risk Management Strategy adopts the priorities set by the Corporate Plan and sets the focus and path to progress attainment of the Value Proposition. The strategy will be revisited each time the Corporate Plan is revised to ensure alignment of focus and priorities, and presented to the Group Risk Committee for endorsement.

Implementation, Stakeholder Engagement and Assurance Plans will be maintained and revisited after each annual maturity evaluation.

Guidelines will be developed, published and maintained to support practice. Standard risk management vocabulary and risk ratings, consequence and likelihood criteria will be applied to support alignment and consistency.

Divisional Risk Management Plans will drive integration, resource provisions and reliable progression to the desired state.

3.5 Capability

3.5.1 Stakeholder Engagement

Effective Stakeholder Engagement is central to building and maintaining risk management capability. This requirement will be incorporated into the broader Risk Management Strategy and revisited annually and adapted if necessary to accommodate emerging conditions and learnings. The business plan for Risk & Assurance will adopt the priorities of the above strategy to provide the capability and resources required to deliver the Risk Management team commitments.

A stakeholder engagement plan will be included in with the Risk Management Strategy to guide implementation.

Each Division will develop their risk management plans including communications and the Risk Management Information System will be used, wherever possible, to satisfy reporting needs.

3.5.2 Training and Competency

Training of staff in risk management is an important part of this Framework. A training strategy that matches skills development with position, accountability and development needs will be implemented and maintained. It will encompass senior and executive managers, Risk Management Coordinators, members of the Board and its relevant committees, project managers and, eventually other employees as required.

AusNet Services will provide:

- Awareness briefings for all staff, including via the company induction training;

- Competency training for Risk Management Coordinators on the Framework, Standards and
- the Risk Management Information System;
- Skills enhancement for facilitators, typically in risk assessment and root-cause analysis;
- Coaching and tools for line manager review and control assurance, design and self-assessment;
- Periodic re-training and continuing professional development of Risk Management Coordinators and other risk management professionals.

The Risk Management Coordinators will be responsible, in association with their human resources support and any training specialists, for drawing up and administering the training plans for their Divisions (part of the overall Divisional Risk Management Plan).

3.5.3 Risk Management Information System (RMIS)

The RMIS provides is at the administrative capability for risk management across the company. Its use will be mandatory to avoid duplication and inconsistent information and reporting. Risk management information should not be stored in spreadsheets or any other systems unless approved by the Manager, Risk and Compliance.

The system will be accessible by all those with a risk management role or accountability for a risk, control or task. All those who are accountable for risks, controls and tasks in the system will require suitable system access. They will also require training and coaching in the use of the system to support their role.

The RMIS will be an accountability driver by:

- Recording risk, control and task owners;
- Prompting risk review, control checking and task completion;
- Recording risk and control checking arrangements;
- Tracking progress on control checking and task completion;
- Producing performance and Governance reports.

RMIS is owned by the Risk Management team. Risk Management Co-ordinators will provide training and support to employees in their divisions. The Risk Management team provide:

- Management of the software installation and upgrades;
- Developing and conducting train-the-trainer and coaching on the system for users;
- Provision of help-desk facilities;
- Adding new users and permissions taking into consideration confidentiality of information;
- Producing reports for reporting defined under section 3.5.4 and report templates;
- Taking system snapshots;
- Creating and changing methodologies and report libraries.

3.5.4 Measuring and Reporting

The reporting on risk will generally be incidental to risk management and not the primary motivation for it.

The principal governance reporting will be to the Executive Leadership Team, Group Risk Committee (GRC) and the Audit and Risk Management Committee (ARMC). Reporting to the GRC will occur quarterly or as required.

The RMIS will play an important role in gathering and enabling the consolidation and reporting of information, in a suitable format, to the GRC and ARMC.

For risk profile reporting, any changes in the risk profile will be highlighted in terms of new material risks, changes in the risk analysis or any changes in control and its effectiveness.

3.6 Accountability

Accountability for risk management will fall into two groups:

- Risk Management Function: delivery of the programs and initiatives associated with establishing or enhancing the risk management framework. This includes planning, resourcing, monitoring and the review of the effectiveness of and therefore continual improvement of its components. The Risk Management team will perform this role in accordance with the stakeholder engagement model and plan;
- Risk Management Practice: Those who are responsible for the application of the risk management process or elements to support decision making in the strategic and day-to-day activities of the company, including Risk, Control and Task Owners, Program and Project Managers.

3.6.1 Governance

The following risk governance structure (Figure 3) has been adopted; it reflects the commitment of AusNet Services to strategic and ongoing risk management Standards:

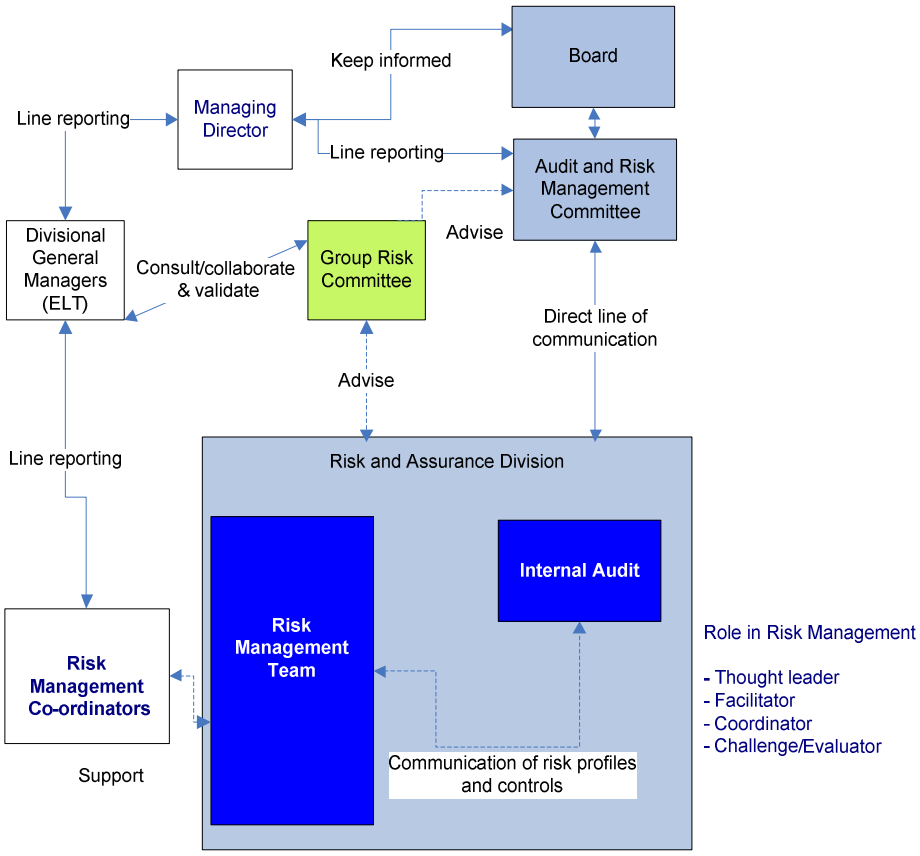


Figure 3 – AusNet Services Risk Governance Model

There are two streams to the risk management governance structure. The first involves assurance to the Board, through independent monitoring and reporting to the Audit & Risk Management Committee (ARMC), of AusNet Services' exposures, risk management effectiveness, and compliance with the Risk Management Policy and Framework. The second involves the Managing Director and business units making decisions and managing risk according to AusNet Services' business objectives, risk tolerance and delegated authorities. Both streams involve reporting.

In the first stream the GRC and ARMC perform oversight roles, and the Risk Management team, create reports to help the Board monitor the risk exposures of AusNet Services. The Risk Management Coordinators assist with this process.

In the second stream, the business unit managers are responsible for risk management and each Division must appoint a Risk Management Coordinator with responsibility for coordinate risk management and for consolidated risk reporting for the Division/Business Units. The Managing Director always retains primary accountability for management of risk within AusNet Services.

Strong and visible commitment to achieving excellence in risk management must be demonstrated through the implementation of a strong risk governance framework supported by robust policies, processes and systems. The governance structure at AusNet Services:

- Defines and endorse the risk management policy;
- Ensures that AusNet Services' culture and risk management policy are aligned;

- Integrates risk management process into decision-making, eg. strategic planning, procurement, project management;
- Ensures legal and regulatory compliance;
- Assigns accountabilities and responsibilities at appropriate levels within AusNet Services;
- Communicates the benefits of risk management to internal and external stakeholders; and
- Ensures that the framework for managing risk remains appropriate.

Accountability is to be assigned, with the commensurate level of authority to execute the responsibilities. The accountabilities will be clearly expressed in terms of what is required, how performance will be measured and how this will count in the overall assessment of an individual's performance. These accountabilities should therefore be part of a particular role and be specified in formal role or position descriptions.

As well as this formal allocation of accountability, as with policy, the company will continually reinforce accountabilities through the normal systems of management: such as in the discussions and the agendas of internal meetings and through the positive reinforcement of good performance. For the same reason, recruitment criteria will take into account the intended risk management accountabilities. Candidates should be required to demonstrate their proficiency in fulfilling such accountabilities with the same emphasis applied as with the other attributes of the role.

Overall risk management responsibilities are specified below. Notwithstanding these responsibilities, and consistent with the principle of accountability, all managers are responsible for identifying, understanding and managing risks consistently with this framework and in conjunction with AusNet Services' Leadership Accountability standards. All employees have a responsibility to understand risk management and attend training as required. It is expected that managers would have key performance indicators to manage risks effectively within their Divisions.

3.6.2 The Board

The Board is ultimately responsible for overseeing the management of risk, as well as approving the strategic direction of the business, annual budgets and business plans and delegations of authority.

The Board has established an Audit & Risk Management Committee to assist in fulfilling its responsibilities, and may delegate responsibilities or authorities described in the Risk Management Framework to this Committee.

3.6.3 Audit & Risk Management Committee (ARMC)

The ARMC has an independent monitoring responsibility to the Board. These responsibilities include:

- To review the Companies' assessment and evaluation of Level I and II risks (significant risks);
- To review and approve the Companies' risk management policies, frameworks and the effectiveness of the implementation of the risk management framework;
- To satisfy itself that management has developed and implemented a sound system of internal control, management of business risks and safeguarding of assets; and

- To satisfy itself that management has developed and implemented a culture of risk management and a system in which there are adequate resources to support the risk management function.

3.6.4 Group Risk Committee (GRC) / (Executive Leadership Team (ELT))

The GRC involves the Managing Director and Divisional General Managers and makes decisions and manages risk in accordance with AusNet Services' business objectives, this framework and delegated authorities. Responsibilities include:

- Reviewing and endorsing the Risk Management Policy, Framework and Strategy;
- Ensuring an effective control environment is in place and that business risks and emerging conditions are identified and monitored;
- Review of reports to be submitted to the ARMC;
- Progress reviews of Divisional risk management plans and the overall implementation of the framework;
- Review of KPIs against targets; and
- Stewardship of the headline risk profile for AusNet Services

3.6.5 Managing Director

The Managing Director always retains primary responsibility for identification and management of risks within the delegations of authority, and the Risk Management Policy and Framework. Supported by the ELT and the GRC, the Managing Director is responsible for ensuring key AusNet Services wide risks that may otherwise not be identified at business unit level are identified and subsequently managed.

The Managing Director provides a statement to the Board in writing together with the Chief Financial Officer, that the statement given in accordance with section 295A of the Corporations Act is founded on a sound system of risk management and internal control which implements the policies adopted by the Board in relation to financial reporting risks, and that the system is operating effectively in all material respects.

The Managing Director may delegate day-to-day responsibilities for risk management to business unit managers, who are expected to make prudent risk and reward decisions for their areas of responsibility and allocate sufficient resources to communicate, identify, analyse, evaluate, treat and report risks.

3.6.6 Chief Financial Officer

The Chief Financial Officer is responsible together with the Managing Director for declaring to the Board in writing that the statement given in accordance with section 295A of the Corporations Act is founded on a sound system of risk management and internal control which implements the policies adopted by the Board in relation to financial reporting risks, and that the system is operating effectively in all material respects.

3.6.7 General Manager, Risk & Assurance

The General Manager, Risk & Assurance reports to the Managing Director and has the day-to-day oversight of risk management.

Responsibilities include:

- Maintaining open communication with ARMC and contacting the Managing Director and the Chairman of the ARMC immediately if a significant risk arises;

- Review of reports to be submitted to the ARMC;
- Reviewing and sponsoring the Risk Management Policy, Framework and Strategy;
- Ensuring an effective control environment is in place and that business risks and emerging conditions are identified and monitored;
- Review of risk management KPIs against targets;
- Fostering a strong culture of risk management throughout AusNet Services in conjunction with the ELT; and
- Develop and implement a system in which there are adequate resources to support the risk management function.

3.6.8 Risk and Control Owners

Risk Owners are responsible for ensuring risk is managed to the degree 'Authority for Continued Toleration of Residual Risk' has been formally given (refer Appendix 1 – Table: Priority for Attention). In addition, Risk Owners are responsible for overseeing the planning, endorsement and progress in implementing risk response strategies, and for escalation to a higher authority if emerging conditions indicate changing risk that may exceed the Authority for Continued Toleration. Risk Owners are obliged to ensure transparency in risk reporting.

Risk owners must ensure that the assessment of risk is up-to-date, reviewed according to the guidelines and is properly recorded in risk registers held in the RMIS.

Control owners need to conduct periodic assurance to check that the controls the company is relying on are in place, effective and cannot be cost-effectively improved.

Task owners will have treatment actions to complete by an agreed date. These tasks can be delegated, but the accountable manager remains fully responsible.

Managers generally will be accountable for the completion and updating of their risk management plans.

3.6.9 Enterprise Program Management Office (EPMO)

The EPMO plays an important role in the risk management of programs within AusNet Services. The EPMO oversees capital investment programs and ensures that effective risk management is undertaken through the application of governance standards including its program methodology, in accordance and consistent with this Risk Management Framework. This responsibility includes ensuring the obligations to prepare and monitor implementation of a project risk control plan and to consult with stakeholders who will bear the impacts of risks or control changes external to the program/project are satisfied.

The EPMO Manager is responsible to ensure an effective, reliable and transparent risk control environment is maintained for the delivery of programs and projects across the organisation through the application of project governance standards.

3.6.10 All Managers

Whilst the Managing Director always retains primary responsibility for identification and management of risks, all managers have a responsibility to:

- Integrate risk management into business processes, eg. Decision-making, procurement, project management, contract management, change management, etc.

- Identify risks and manage those risks for which they have been declared the Risk Owner and escalate Level I, II and III risks to General Managers and above as per the 'Priority for Attention' Table set out in Appendix 1. This includes managing the risk by ensuring that controls and treatment actions are included in the budget process;
- Ensure that all employees are aware of expected principles of behaviour as embodied in the Risk Management Framework; and
- Ensure all employees are encouraged to report, and remedy violations of those principles.

3.6.11 Employees

All employees are responsible for:

- Adherence to the Risk Management Policy and Framework;
- Communicating emerging conditions and risks to line management;
- Being aware of risks and acting on or escalation of risks as required; and
- Attending risk management training as required.

3.6.12 Manager, Risk and Compliance and Risk Management Team

The Manager, Risk and Compliance leads the Risk Management team and reports to the General Manager, Risk and Assurance. The Manager, Risk and Compliance also has access to the Managing Director, the ARMC, and ultimately the Board, and is responsible for providing risk management reports. This arrangement supports the independent nature of those specific responsibilities.

Generally the Risk Management team will not be tasked with day-to-day risk assessment activities but provide strategic direction and coordination of:

- Risk management generally;
- Supporting the Risk Management Co-ordinators with technical advice;
- Consistency in analysis, evaluation, monitoring & reporting between divisions;
- Enterprise wide analysis;
- Project risk management in conjunction with the EPMO; and
- Governance reporting.

Specifically the Manager, Risk and Compliance will be responsible for:

- Maintaining the company Risk Management Framework and Standards;
- Developing draft guidelines for review;
- Supporting the framework and guidelines through the provision of training and coaching;
- Hosting and maintaining the RMIS;
- Analysing risk management reports and compiling summary reports to the GRC and ARMC;
- Fostering a strong Risk Management culture throughout the company.

While the Risk Management team will work closely with assurance providers such as Internal Audit, they will not undertake assurance activities so as to avoid conflicts of interest.

3.6.13 Risk Management Coordinators

The General Managers of each Division shall be responsible for appointing Divisional Risk Management Coordinator/s who are responsible for the following within their Division:

- Assisting with implementation of the risk management framework, policy and guidelines through a top-down process of engagement;
- Conducting risk assessments;
- Acting as custodians of their risk management plans;
- Taking the initiative to embed risk management processes into key processes, including strategic and business plan development;
- Compiling divisional reports as required;
- Liaising with Internal Audit and other assurance providers;
- Maintaining and updating risk registers (based on the consolidation and rolling-up of subordinate risk registers) in the RMIS;
- Developing training plans and support for risk management;
- Fostering a strong Risk Management culture throughout their area; and
- Undertaking relevant risk management training as required.

3.6.14 Internal Audit

The General Manager, Risk and Assurance administratively reports to the Managing Director and reports to the ARMC on the effectiveness of risk management and the internal controls system. As both risk management and internal audit functions reports to the General Manager, Risk & Assurance, Internal Audit shall appoint an external provider to review the effectiveness of the overall Risk Management Framework, including the activities of the Risk Management team, and report to the Managing Director, ARMC and the Board as required. This will ensure independence due to the line reporting of risk management. Internal Audit will provide validation utilising the risk management maturity evaluation protocol.

3.7 Continual Improvement

The risk management framework is largely self-regulating. The focus of the continual improvement strategy will be to provide assurance about whether the risk management framework as a whole is effective and is being implemented correctly. This will include:

- Control assurance will be undertaken by Risk and Control Owners using control self-assessment. Internal Audit will have the role of providing formal assurance. Internal Audit will also monitor and evaluate regularly the effectiveness of the company's risk management framework.
- Guidance for Divisions to develop plans that reflect its decisions on the pace and targets for integration, against which its progress will be monitored and reported to the GRC;
- The use of the RMIS with appropriate functionality to support consistency and to allow efficient monitoring and reporting; and

- Provisions for training and mentoring to the required level of competence, so that they can fulfil their responsibilities for managing risk.

3.7.1 Performance Criteria

To drive forward risk management, it will be necessary to set performance measures (KPIs) and goals against which progress can be measured. These will largely be lead measures to encourage the take-up of good risk management practices and to achieve completion of divisional risk management plan actions.

The performance measures will be aligned with the Leadership Accountability Standards. They will be linked to and integrated into the current performance management process in the company.

Generically, the Risk Management Standards will set company-wide performance criteria for:

- Integrating risk management into decision making;
- Integrating risk management into planning, including stakeholder engagement;
- Post-event analysis and lessons learned from successes and failures;
- The active and systematic assurance of controls;
- The analysis and prioritisation of risks and controls;
- Risk evaluation;
- Risk treatment;
- Handling risk management information;
- Governance reporting;
- Resources for risk management.

The improvement in risk management maturity is an important lead measure that can be linked to performance management systems and used to focus management attention on the area for improvement.

3.7.2 Risk Management Maturity Evaluation

AusNet Services will use a formal system to measure and report the maturity of its approaches to the management of risk and its improvement over time. Such a system will provide an important contribution to governance reporting and will help to focus line management attention on their accountability for compliance with the company risk management policy and Standards.

The areas of focus initially are:

- Assessment of the risks associated with changes and decisions;
- Project risk management;
- Assurance of key controls;
- Systematic learning from successes and failures; and
- Assurance of strategies for dealing with disruption related risks.

Most importantly, Divisions should undertake the maturity evaluation so that the reports submitted by each Division to the GRC and ARMC accurately reflect performance and the management team

accountability for that performance. The evaluation will be conducted once a year to provide the ARMC with an accurate representation of the effectiveness of the implementation of the framework.

A risk management maturity evaluation will be the starting point in each Division for the development of its risk management plan. These plans will respond to the gaps revealed by the evaluation. The annual re-evaluation will then become the opportunity to revise and re-focus the plans.

3.7.3 Control Assurance

Control assurance will principally be through the use of control self-assessment, practiced by control owners on key controls. The Risk Management Information System will support this where possible.

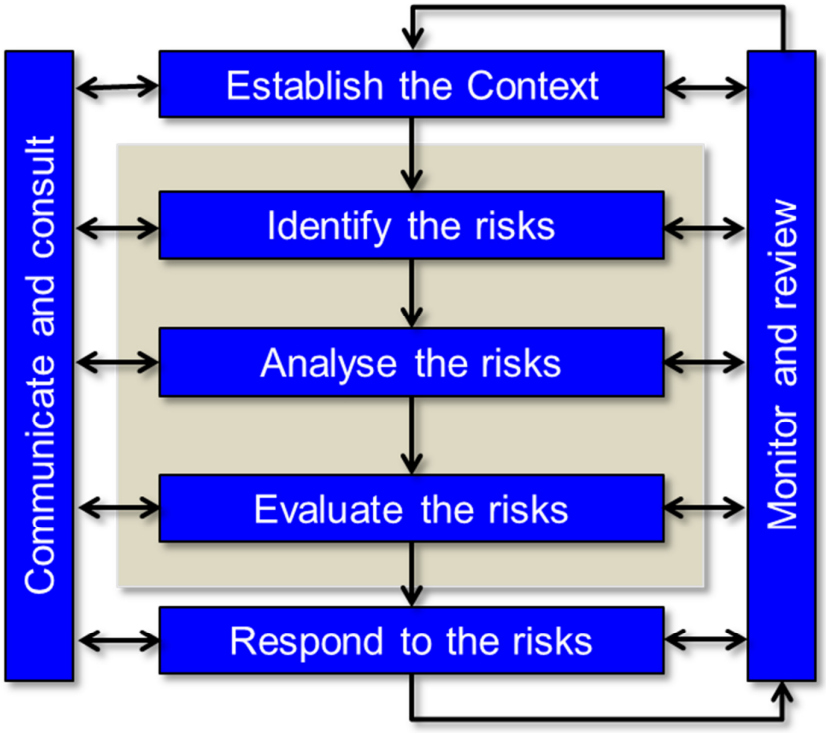
A key measure within the qualitative risk analysis approach specified under the risk management Standards will be control effectiveness (RCE). Control assurance will focus on validating this measure in terms of both the adequacy and effectiveness of controls.

4. RISK MANAGEMENT PROCESS

4.1 The Risk Management Process Overview

AusNet Services has adopted the risk management process as detailed in AS/NZS ISO 31000 (see **Figure 1**). All steps in the process will be applied. Detailed guidance on its application will be given in the Risk Assessment and Treatment Guidelines.

Figure 1: Risk management process



Specific requirements and guidance is further detailed in separate guidelines.

4.2 Risk Documentation

With each step in the risk process, adequate documentation should be evident, including but not limited to assumptions, methods, data sources and results. The RMIS is utilised for capturing this information and the development of reports such as the Corporate Risk Profile and Risk Treatment Actions.

Integration with Business Planning and Strategy

Risk Management is embedded into Business and Strategic planning and decision making to ensure risks in achieving planned objectives are recognised and plans stress-tested. This takes the form of an operating environment scan, identifying emerging conditions, whether threats or opportunities, and undertaking a preliminary assessment of the potential to impact on planned objectives.

The preliminary assessment includes determining if it is an emerging risk, or an emerging condition which may influence an existing risk. Sensitivity and/or scenario analysis may be used to further analyse break points, where dependency is assumed, and constraints that may emanate from these uncertainties.

The risks deemed a priority for action and/or monitoring for emerging conditions will be placed in the RMIS for monitoring and reporting.

It is beneficial to invest time identifying emerging conditions and 'Black Swan' risks to understand the changing environment, recognise risk interdependencies and any constraints and vulnerabilities that limit downside impacts and avoid surprises. It also enables better informed decisions making and ultimately improves resilience of AusNet Services.

4.3 Emerging Conditions

Emerging conditions (external and internal) that have been identified which may have an impact on the organisation in the longer term should be immediately reported to the General Manager of the Division and the Risk Management team.

The General Manager should seek assistance (if required) from their Risk Management Coordinator to perform a risk review of the relevant risk(s) with regard to the implications of the emerging condition and to what degree the existing control environment will address the change. The risk assessment record in the RMIS should be updated accordingly, including adding comments outlining the evaluation of the emerging condition(s), in the RMIS as normal practice.

In addition, General Managers should communicate emerging risks at the Group Risk Committee where the Committee will conduct further analysis and make a decision on the materiality of the risk and whether a more detailed analysis is to be performed.

General Manager, Risk & Assurance and the Managing Director are responsible for updating the ARMC and the Board if the emerging risk is considered materially significant, or likely to have a negative impact on reputation.

4.4 Black Swan Risks

'Black Swan' risks are unforeseen, significantly disruptive events or conditions. These are characterised as high potential severity, low likelihood situations, and often involve long-tailed and/or fat-tailed events. They are usually complex and often result in being extremely difficult to predict when and what the degree and span of potential impacts may be.

Similar to emerging conditions, where a 'Black Swan' risk is suspected, immediate action should be to undertake a preliminary analysis and determine if it is already in the scope of an existing risk assessment or is a previously unidentified, business critical risk. Immediate notification of these risks is also required consistent with the normal escalation protocols, as outlined in the next section. A more robust assessment can then be carried out, with the key stakeholders and decision makers' contributions. With regards to treatment of these risks, the general advice is that since they are unpredictable, it is necessary to accept their existence and invest in preparedness rather than prediction, with the aim of preparing for the impact and strengthening the ability to anticipate and detect trends before they evolve into full-blown Black Swan events.

5. COMPLIANCE WITH THE RISK MANAGEMENT FRAMEWORK

Employees and contractors must comply with both the letter and the spirit of the Risk Management Policy and Framework at all times. AusNet Services' Code of Business Conduct establishes the requirement to comply with all policies and procedures. Any activities considered to be in conflict with the Risk Management Framework are considered to be a breach and treated as set out in the section below.

The Managing Director and the Executive Leadership Team are responsible for implementing, integrating, and ensuring compliance with the framework throughout AusNet Services. The ARMC assisted by the Risk Management team, Internal Audit and other support functions will independently monitor the compliance with AusNet Services' Risk Management Policy and Framework.

5.1 Breaches

Failure to abide by the mandated requirements in the Risk Management Framework constitutes a breach of policy. Failure to report a breach is itself a breach.

Activities in breach of the Risk Management Policy and Framework may result in disciplinary action, including termination of employment, consistent with the Code of Business Conduct.

When a breach is identified, it must be dealt with in accordance with the following process:

- It must be notified immediately to the relevant General Manager and the Risk Management Coordinator, who are jointly responsible for notifying the Manager, Risk and Compliance.
- The Manager with responsibility for that risk will prepare a summary of events leading to the breach and, if relevant, recommend actions to remedy the breach and restore compliance with policy.
- If it is a breach of policy limits or otherwise represents a material risk to AusNet Services, the Risk Management team may recommend additional or modified remedial actions to the General Manager, who is not obliged to accept the recommendations.
- If the Manager, Risk and Compliance is not able to establish that appropriate remedial measures have been taken, these concerns will be communicated to the Managing Director who will determine the appropriate course of action.
- General Managers must ensure any material breach relating to a Level I risk is reported to the Managing Director and General Manager, Risk & Assurance and subsequently to the Chairman of the ARMC immediately and then to the next ARMC meeting along with results of any remedial actions taken and any assessments made by the Manager, Risk and Compliance.
- Violations of policy limits are to continue to be reported as a breach of policy until such time as compliance with policy is restored.
- The Risk Management team will enter it in a register of breach notifications that it must maintain.

Uncertainty about this process is to be referred to the Risk Management team for clarification. Open communication is encouraged.

6. FRAMEWORK ADMINISTRATION

6.1 Access to the Risk Management Framework

The Risk Management Framework is available on AusNet Services' intranet or by contacting a member of the Risk Management team. Restricted access to documents that include confidential information will be considered on a case-by-case basis.

6.2 Authority to Approve and Amend Framework

The Group Risk Committee, (GRC), initially endorses the Risk Management Framework and is authorised to amend the Risk Management Framework. Final approval of the ARMC to implement the amended Risk Management Framework is required.

Any employee may propose an amendment to the Risk Management Framework. Normally, a suggested amendment will be proposed through the relevant Manager or General Manager of that area, who will consult with the Manager, Risk and Compliance.

The Manager, Risk and Compliance will review the proposal and, if requested, assist with the preparation of a detailed recommendation.

The GRC will ensure that adequate analysis and consultation has taken place. The GRC will consider the assessments made by the Risk Management team when considering the recommendation.

6.3 Review

Each year the Manager, Risk and Compliance will conduct a self-assessment of the risk management framework, its alignment with business strategy and priorities and its state of implementation. This will include the analysis of the successes and failures of the previous year and the lessons learnt. This review will be reported to the GRC and ARMC. If required, changes will be made to the company framework after this review. Generally, it is expected that the Framework will be reasonably stable and addition or adjustments to Practice Guides may be used to supplement detailed requirements.

At least every three years the GRC is to undertake a formal review of the Risk Management Framework to consider the alignment of the Framework to the business priorities, the appropriateness of the Framework, and the effectiveness and efficiency of risk management in AusNet Services. The Risk Management team and other internal and external resources will assist the GRC, as considered necessary. If the ARMC or the GRC observe significant difficulties in abiding by the Risk Management Framework (including risk tolerances and operational thresholds) they must initiate a review as soon as practicable.

6.4 Document Authorisation, History and Maintenance Record

Authorisation:

	Name	Date
Updated by	Priscilla Taylor, Manager, Risk & Compliance	February 2013
Reviewed by	Claire Hamilton, General Manager, Risk & Assurance	February 2013
Endorsed by	Group Risk Committee	25 February 2013
Approved by	Audit and Risk Management Committee	

History:

Version	Date	Approved by:	Description
1.0	1 December 2005	Group Risk Committee	Initial GRC approval
1.0	15 February 2006	Audit & Risk Management Committee	Initial ARMC approval
2.0	14 August 2007	Group Risk Committee	Approval
3.0	10 December 2009	Group Risk Committee	Endorsement
3.0	10 February 2010	Audit and Risk Management Committee	Approval
4.0	25 February 2013	Group Risk Committee	Endorsement
4.0	27 March 2013	Audit & Risk Management Committee	27 March 2013

Maintenance requirements:

Revision frequency	Every three years
Revision Responsibility	Manager, Risk and Compliance
Additional triggers	Changes in business model, Risk Management Policy or Strategy