Overview of Risk & Compliance Management

for the Australian Energy Regulator (AER)

AusNet services

Elaine Carlin, Risk & Assurance

30 April 2015

mission zero

Agenda

- Objectives
- Definition of Risk
- Methodology & Framework
- Governance Structure
- Risk & Compliance Process
- Risk Assessment Tools
- Information Management Systems (Cura & CMS)
- Questions?

Objectives

To provide an overview and awareness of the AusNet Services:

- Risk Management Framework & Methodology,
- Risk Management Information System (Cura),
- Compliance Management Framework & Methodology, and
- Compliance Management System (CMS)

and for you to obtain an understanding of how we assess and manage risks / obligations within the business.

What is Risk?

- **"Effect of uncertainty on objectives"** (ISO 31000:2009)
  - An effect may be positive, negative, or a deviation from the expected.
  - An objective may be financial, related to health and safety, or defined in other terms and can apply at different levels (e.g. strategic or process level).
  - Risk is often described by reference to potential events and consequences.
  - Risk can be expressed in terms of a combination of the consequences of an event or a change in circumstances, and their likelihood of occurring.
- **Risk management** can be defined as the "coordinated activities to direct and control an organisation with regard to risk" (ISO 31000:2009).

Methodology & Framework

RISK MANAGEMENT

Has been designed based on:

- ISO 31000:2009 - Risk Management – Principles and Guidelines.

Key reference documents:

- Risk Management Policy (2013)
- Risk Management Framework (2013)
- Risk Management Guide (2009 – currently under revision)
- Risk Management Practice Guides (2015)
- E-learning module (2010)

COMPLIANCE MANAGEMENT

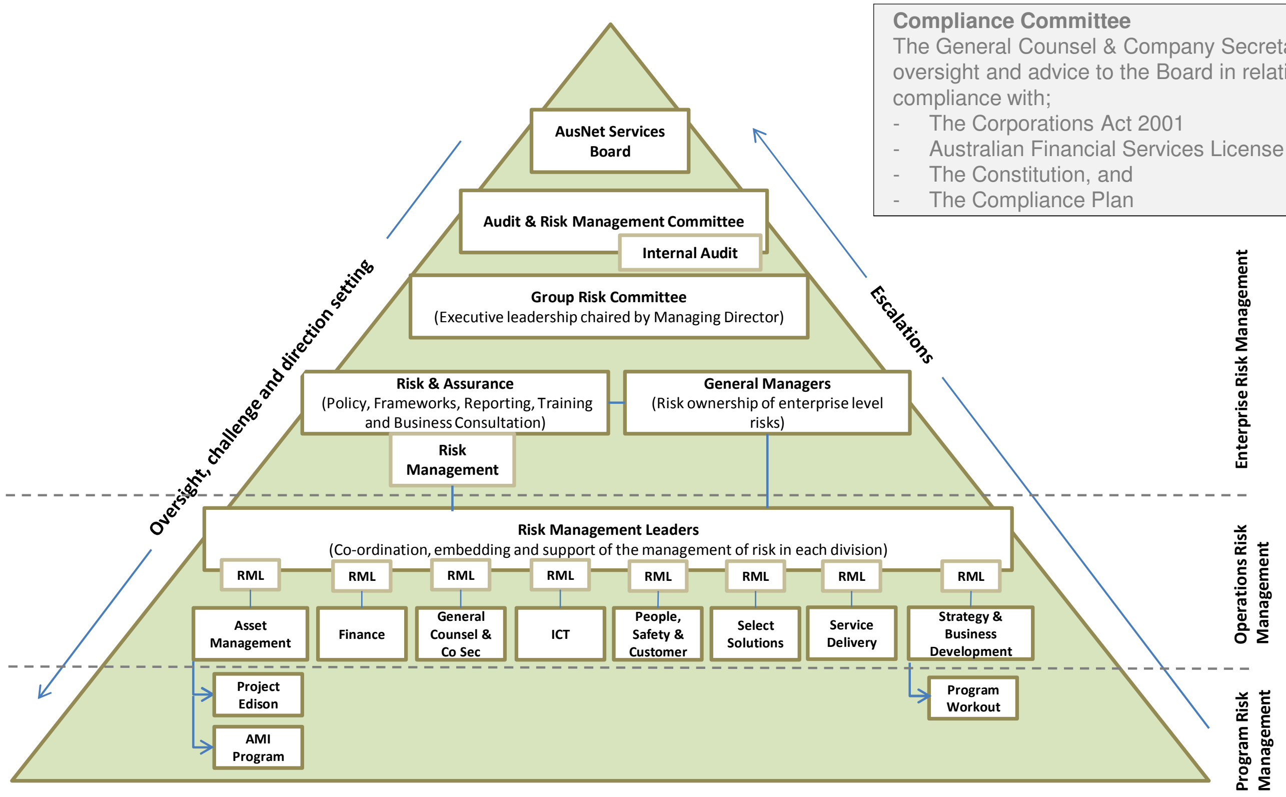
Has been designed based on:

- AS3806:2006 - Compliance Programs.
- To be reviewed and aligned with ISO 19600 in 2015/16.

Key reference documents:

- Code of Business Conduct (2014)
- Corporate Compliance Policy Statement (2014)
- Corporate Compliance Framework (2013)
- Risk Management Guide (2009 – currently under revision)
- Breach Notification Form (2013)

Governance Structure



AusNet Services Board

Audit & Risk Management Committee

Internal Audit

Group Risk Committee
(Executive leadership chaired by Managing Director)

Risk & Assurance
(Policy, Frameworks, Reporting, Training and Business Consultation)

Risk Management

General Managers
(Risk ownership of enterprise level risks)

Risk Management Leaders
(Co-ordination, embedding and support of the management of risk in each division)

RML — Asset Management

RML — Finance

RML — General Counsel & Co Sec

RML — ICT

RML — People, Safety & Customer

RML — Select Solutions

RML — Service Delivery

RML — Strategy & Business Development

Project Edison

AMI Program

Program Workout

Oversight, challenge and direction setting

Escalations

Enterprise Risk Management

Operations Risk Management

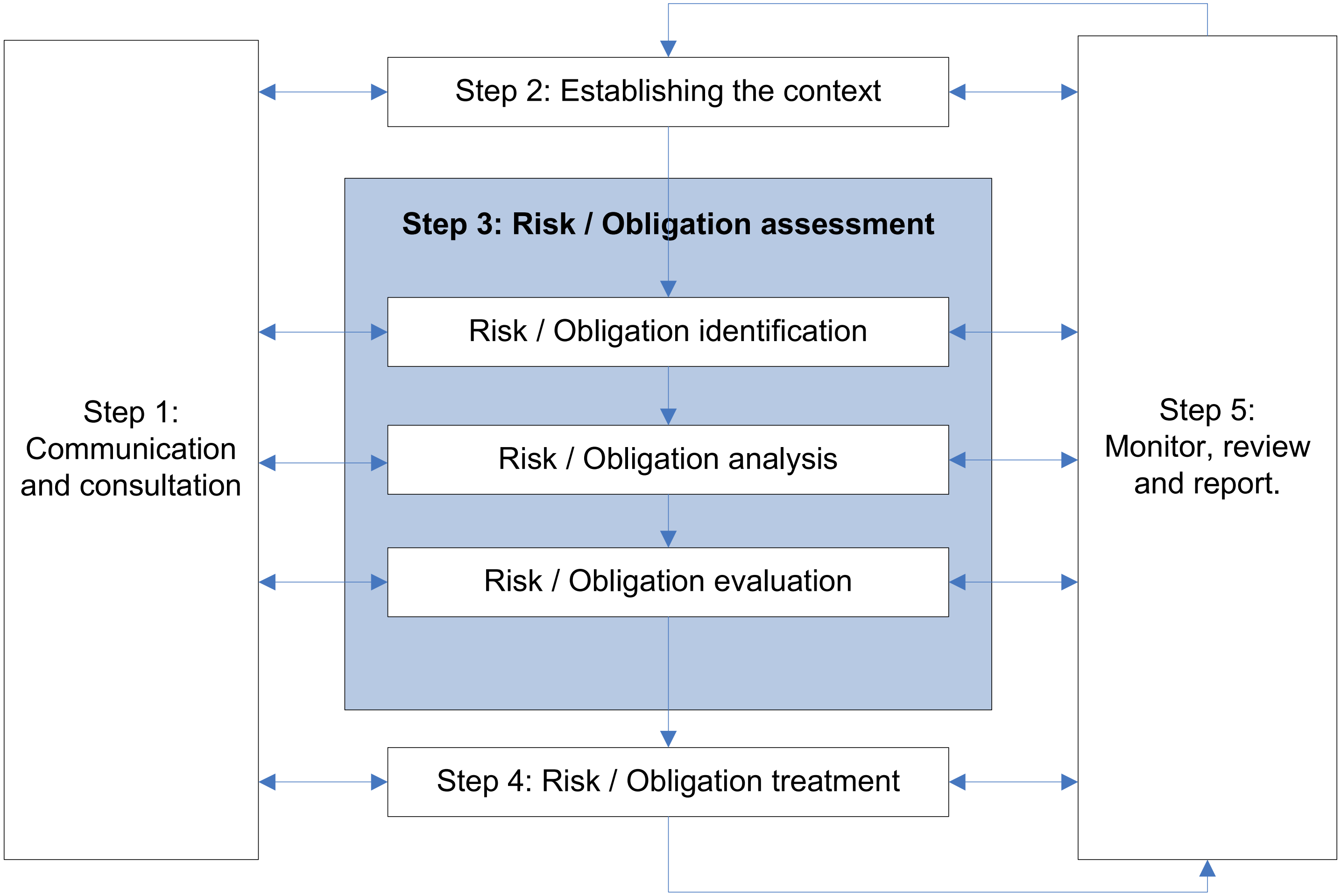
Program Risk Management

Compliance Committee

The General Counsel & Company Secretarial Division provide specific oversight and advice to the Board in relation to the Responsible Entity's compliance with;

- The Corporations Act 2001
- Australian Financial Services License
- The Constitution, and
- The Compliance Plan

Risk & Compliance Process


Step 1: Communication and consultation

Step 2: Establishing the context

Step 3: Risk / Obligation assessment

Risk / Obligation identification

Risk / Obligation analysis

Risk / Obligation evaluation

Step 4: Risk / Obligation treatment

Step 5: Monitor, review and report.

Risk & Compliance Steps

Step 1 Communication and Consultation

- Communication and consultation with internal and external stakeholders as far as necessary should take place at each stage of the risk and compliance management process.

Step 2 Establishing the Context

- Establishing the context defines the basic parameters for managing risks and obligations and sets the scope and criteria for the rest of the risk and compliance management process.
- The overall risk / obligation assessment process occurs within the structure of an organisation’s external, internal and risk management context.

Risk & Compliance Steps

- **Step 3 Risk Assessment**
- **Risk Identification *(finding, recognising, and describing risks)***

- Aim is to **generate a comprehensive list** of risks based on those events and circumstances that might impact (enhance, prevent, degrade or delay) the achievement of business objectives.
- Risks are typically identified by employees at all levels.
- Identification of risks may occur through team workshops, one-on-one interviews, or control self-assessment (sources of risk).
- A focus on emerging risks.

Step 3 Compliance Risk Assessment

Obligation risk ratings *(finding, recognising, and describing risks)*

- Compliance obligations are allocated to employees 'Responsible Persons' (RPs) whose roles are best placed to provide assurance as to the status of compliance on an ongoing basis.
- Risk ratings applied to obligations may be 'prescribed' by a regulator or 'non-prescribed' in which case the AusNet Services 'Risk Management Guide' is utilised.
- Non-prescribed risks ratings are typically allocated by 'Responsible Persons' with oversight from specialist compliance resources.
- A focus is on monitoring obligations to which a high risk / market impact is attached.

Risk & Compliance Steps

Risk Analysis ***(nature and level of risk)***

- Risk analysis is about **developing an understanding of the risk** and its nature. It provides an input to risk evaluation and to decisions on whether risks need to be treated and the most appropriate treatment strategies.

- This involves analysing risks in terms of **consequence and likelihood**.

- Existing **risk controls and their effectiveness** should be taken into consideration (residual rating).

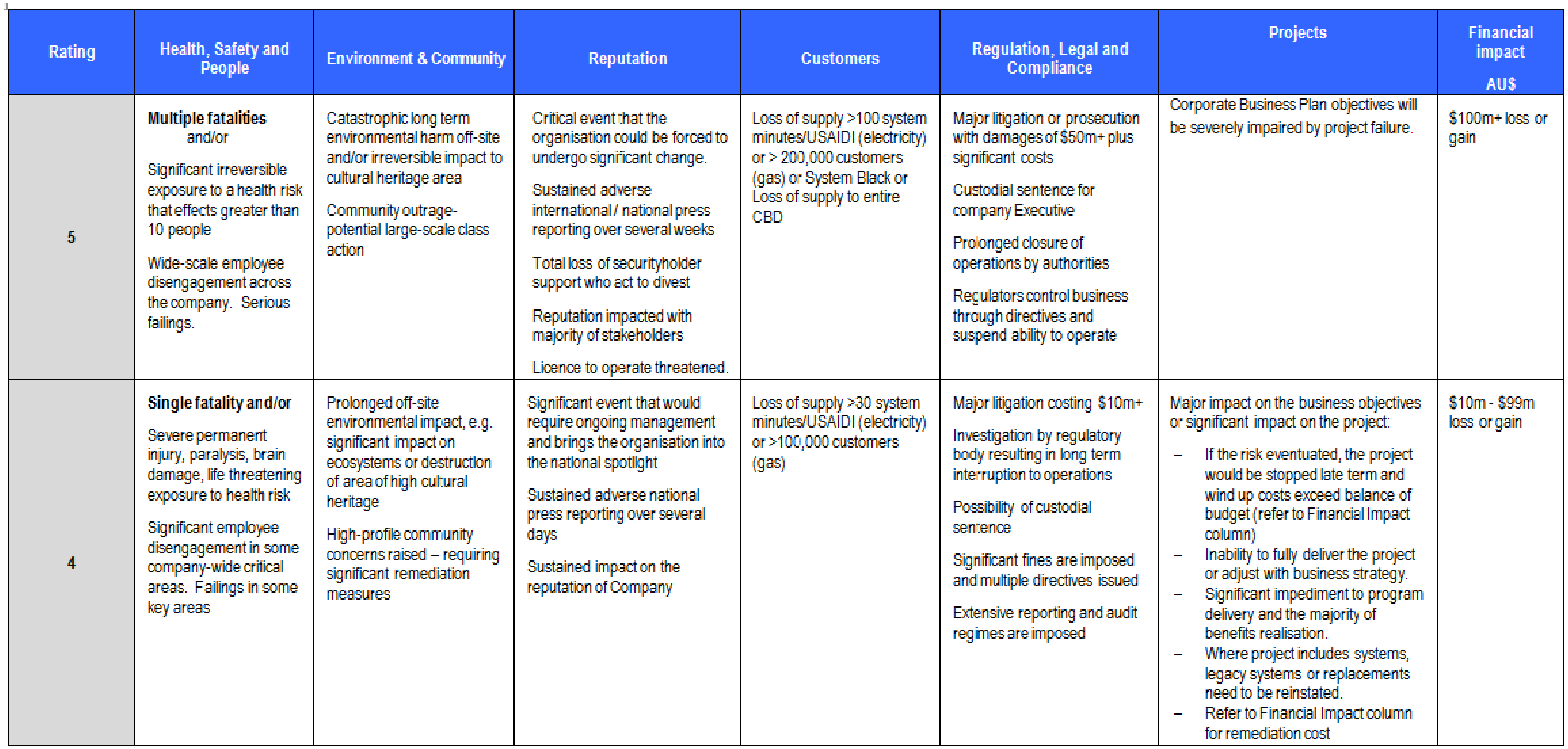
- Analysis may be undertaken to **various degrees of detail** (qualitative, semi-quantitative and quantitative).

- Best to do a **qualitative analysis first** to obtain a more general indication of the level of risk.

- Whilst the focus on risk tends to be on negative consequences, it is important to consider the **risks associated with not pursuing an opportunity.**

Consequence Criteria

- A consequence rating should be chosen on the basis of the expected consequences on AusNet Services and its stakeholders after considering the current control environment. If there are consequences over a number of different types, then the highest level of the consequence types should be chosen. The table below is based on the Risk Assessment Framework.



Rating	Health, Safety and People	Environment & Community	Reputation	Customers	Regulation, Legal and Compliance	Projects	Financial impact AU$
5	**Multiple fatalities** and/or Significant irreversible exposure to a health risk that effects greater than 10 people Wide-scale employee disengagement across the company. Serious failings.	Catastrophic long term environmental harm off-site and/or irreversible impact to cultural heritage area Community outrage- potential large-scale class action	Critical event that the organisation could be forced to undergo significant change. Sustained adverse international / national press reporting over several weeks Total loss of securityholder support who act to divest Reputation impacted with majority of stakeholders Licence to operate threatened.	Loss of supply >100 system minutes/USAIDI (electricity) or > 200,000 customers (gas) or System Black or Loss of supply to entire CBD	Major litigation or prosecution with damages of $50m+ plus significant costs Custodial sentence for company Executive Prolonged closure of operations by authorities Regulators control business through directives and suspend ability to operate	Corporate Business Plan objectives will be severely impaired by project failure.	$100m+ loss or gain
4	**Single fatality and/or** Severe permanent injury, paralysis, brain damage, life threatening exposure to health risk Significant employee disengagement in some company-wide critical areas. Failings in some key areas	Prolonged off-site environmental impact, e.g. significant impact on ecosystems or destruction of area of high cultural heritage High-profile community concerns raised – requiring significant remediation measures	Significant event that would require ongoing management and brings the organisation into the national spotlight Sustained adverse national press reporting over several days Sustained impact on the reputation of Company	Loss of supply >30 system minutes/USAIDI (electricity) or >100,000 customers (gas)	Major litigation costing $10m+ Investigation by regulatory body resulting in long term interruption to operations Possibility of custodial sentence Significant fines are imposed and multiple directives issued Extensive reporting and audit regimes are imposed	Major impact on the business objectives or significant impact on the project: – If the risk eventuated, the project would be stopped late term and wind up costs exceed balance of budget (refer to Financial Impact column) – Inability to fully deliver the project or adjust with business strategy. – Significant impediment to program delivery and the majority of benefits realisation. – Where project includes systems, legacy systems or replacements need to be reinstated. – Refer to Financial Impact column for remediation cost	$10m - $99m loss or gain

Consequence Criteria

Rating	Health, Safety and People	Environment & Community	Reputation	Customers	Regulation, Legal and Compliance	Projects	Financial impact AU$
3	**Serious Injury** Moderate permanent effects from injury or exposure. For example, serious burns, serious internal and/or head injuries, gassings that require hospitalisation Significant employee disengagement or failures in non-critical areas	Major event leading to local on and off-site impact on ecology or damage to area of cultural heritage Medium term recovery High potential for complaints from interested parties	Major event that causes adverse local press reporting over several days Reputation impacted with some stakeholders	Loss of supply >10 system minutes/USAIDI (electricity) or >5,000 customers (gas)	Major breach of law with punitive fine Significant litigation involving many weeks of senior management time Fines imposed, directive issued and additional audit and reporting requirements	Moderate impact on the business objectives or on the project: – Will cause major replan of project and revision of scope, cost, schedule and resources - Inability to substantially deliver the program or adjust with strategy change - partially realised benefits - Where project includes systems, legacy systems remain. - Refer to Financial Impact column for remediation cost	$1m – $9m loss or gain
2	**Significant injury** Medically treated injuries from which recovery is likely. For example, burns, broken bones, severe bruises, cuts, etc. Minor employee disengagement and failures in non-critical areas	Medium term recovery, immaterial effect on environment/ community required to inform Environmental agencies, (e.g.: noise, dust, odour)	Adverse local press reporting Reputation impacted with a small number of stakeholders	Loss of supply >3 system minutes/USAIDI (electricity) or >500 customers (gas).	Breach of law with investigation or report to authority with prosecution and/or moderate fine possible Specific regulatory audit with critical findings and recommended actions	Minor impact on the business objectives or on the project: – Inability to partially deliver the program or adjust with strategy change – May impact tasks on the critical path – May impact tasks with dependencies external to project – Most key benefits will be realised – Refer to Financial Impact column for costs.	$100k – $999k loss or gain
1	**Minor injury** No medical treatment. For example, cuts, bruises, no measurable physical effects Short-term loss of morale in non-critical areas	Small, unconfined event, no impact on ecology or area of cultural heritage Short term transient environmental or community impact- little action required	No press reporting or external interest	Loss of supply >1 system minute/USAIDI (electricity) or >100 customers (gas)	Minor legal issues, non-compliances and statutory fine Routine regulatory reporting and audits	Insignificant impact on the business objectives or on the project: – Doesn't impact the ability to deliver the program or adjust with strategy. – Doesn't impact tasks on the critical path – Doesn't impact tasks with dependencies external to the project – Benefits can still be realised – Refer to Financial Impact column for costs.	< $99k loss or gain

Likelihood Criteria

A likelihood category should be chosen on the basis of the chance that AusNet Services or its stakeholders could be affected at the chosen level of consequence. For example, the chance of loss of supply of >1 system minute (electricity distribution) every time a storm occurs in the Dandenong ranges may be a 99% probability.

Rating	Criteria
E	• Impact is occurring now, or • Could occur within “days to weeks”, or • >99% probability
D	• Balance of probability will occur, or • Could occur within “weeks to months”, or • >50% probability
C	• May occur shortly but a distinct probability it won’t, or • Could occur within “months to years”, or • >20% probability
B	• May occur but not anticipated, or • Could occur in “years to decades”, or • >1% probability
A	• Occurrence requires exceptional circumstances • Exceptionally unlikely, even in the long term future • Only occur as a “100 year event”, or • <1% probability

Risk Control Effectiveness

The relative assessment of actual level of control that is currently present and effective compared with that reasonably achievable for that particular risk. RCE will therefore be an indicator as to whether AusNet Services is doing all that it could or should to manage the risk issue.

RCE	Guide	Indicators
Fully Effective	Nothing more to be done except review and monitor the existing controls Controls are well designed for the risk, address the root causes and management believes that they are **effective** and reliable at all times. Control is deemed to be operational in excess of 95% of the time	The control is: • Designed appropriately to meet its objectives • Operating as anticipated at all times • Documented and accessible • Communicated to and understood by relevant persons • Reviewed on a regular basis (at least annually) & updated when necessary • Approved by the relevant Committee • Reviewed as part of the Internal Audit (IA) process and no issues were identified
Substantially Effective	Most controls are designed correctly and are in place and effective . Some more work to be done to improve operating effectiveness or management has doubts about operational effectiveness and reliability Control is deemed to be operational between 75% and 94% of the time	The control is: • Designed appropriately to meet its objectives • Operating as anticipated the majority of the time • Documented and accessible • Communicated to and understood by relevant persons • Reviewed on a regular basis (at least annually) but may not be updated when necessary • Approved by the relevant Committee • Reviewed as part of the IA process and only low rated issues were identified
Partially effective	Whilst the design of controls may be 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 seem correctly designed in that they do not treat root causes, those that are correctly designed are operating effectively Control is deemed to be operational between 50% and 74% of the time	The control is: • Designed appropriately to meet the majority of objectives • Operating as anticipated some of the time • Documented and accessible • Communicated to relevant persons • Reviewed on an ad hoc basis and may or may not be updated when necessary • Approved by the relevant Committee • Reviewed as part of the IA process and medium issues were identified or not reviewed as part of the IA
Largely ineffective	Significant control gaps. Either controls do not treat root causes or they do not operate at all effectively. Control is deemed to be operational between 25% and 49% of the time	The control is: • Not designed appropriately to meet the majority of objectives • Not operating as anticipated at any time • Documented but not accessible • Not communicated and understood by relevant persons • Not reviewed on a regular basis (at least annually) or updated when necessary • Not approved by the relevant Committee • Reviewed as part of the IA process and medium to high rated issues were identified or not reviewed as part of the IA
None or totally ineffective	Virtually no credible control. Management has no confidence that any degree of control is being achieved due to poor control design and/or very limited operational effectiveness Alternatively, the risk is new and controls are yet to be implemented If any control exists it would be operational less than 25% of the time	The control is: • Not designed appropriately to meet its objectives • Not operating as anticipated at any time • Not documented or accessible • Not communicated and understood by relevant persons • Not reviewed on a regular basis (at least annually) or updated when necessary • Not approved by the relevant Committee • Reviewed as part of the IA process and high rated issues were identified or not in existence

Risk & Compliance Steps

Evaluate Risks (comparing the results of risk analysis)

- The purpose of risk evaluation is to assist in making decisions, based on the outcomes of risk analysis, about which risks need treatment and treatment priorities.

- The decision to tolerate a risk should be based on a consideration of:
  - ➢ Whether the risk is being controlled to a level that is reasonably achievable,
  - ➢ Whether it would be cost-effective to further treat the risk, and
  - ➢ AusNet Service's willingness to tolerate risks of that type.

Risk Matrix

The matrix should be used to determine the priority of attention to the risk

Consequences	5	II	II	I	I	I
	4	III	II	II	I	I
	3	III	III	II	II	I
	2	IV	III	III	II	II
	1	IV	IV	III	III	III
		A	B	C	D	E
		Likelihood				

The decision to tolerate a risk should be based on a consideration of:

- Whether the risk is being controlled to a level that is reasonably achievable;
- Whether it would be cost-effective to further treat the risk; and
- AusNet Service's willingness to tolerate risks of that type.

Risks rated as Level IV (low risks) or tolerable risks may be accepted with minimal further treatment. They will be monitored and periodically reviewed to ensure they remain so. If risks are not judged low or tolerable, they should be treated.

Priority for Attention

Priority for attention and the seniority of management sign-off for continued toleration of risks will be as shown below.

Residual risk level	Suggested action	Suggested timing	Authority for continued toleration of residual risk
I	Take immediate action to treat risk.	Short term. Action Plans prepared and normally implemented within 1 month.	Board (ARMC)
II	Plan to deal with in keeping with the business plan.	Medium term. Action Plans prepared and normally implemented within 6 months.	Managing Director
III	Plan in keeping with all other priorities.	Action Plans prepared and normally implemented within 1 year	General Managers
IV	Will still require attention within existing operations.	Ongoing control as part of a management system.	Managers

Risk & Compliance Steps

Step 4 Risk Treatment *(process to modify risk)*

- Risk treatment involves identifying a **range of options for treating risks**, evaluating these options, preparing treatment plans and implementing them.

- Risks that do not have effective controls in place require action to reduce the risk to an acceptable level. There are seven methods of treating risks:
  - ➢ Avoid 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, and
  - ➢ Retaining the risk, either by choice or by default.

- Concept of **Target Risk**: What is the risk level potentially achievable after future controls are in place?

Risk & Compliance Steps

Step 5 Monitor, Review and Report.

- All risks / obligations are to be **monitored and reviewed** on a ongoing basis to ensure that:
  - The risk / obligation controls remain effective, and
  - The treatment plans remain effective in both design and operation.

Information Management Systems

Risk Management

- **CURA is used to capture, maintain and report on risks managed throughout the business.**

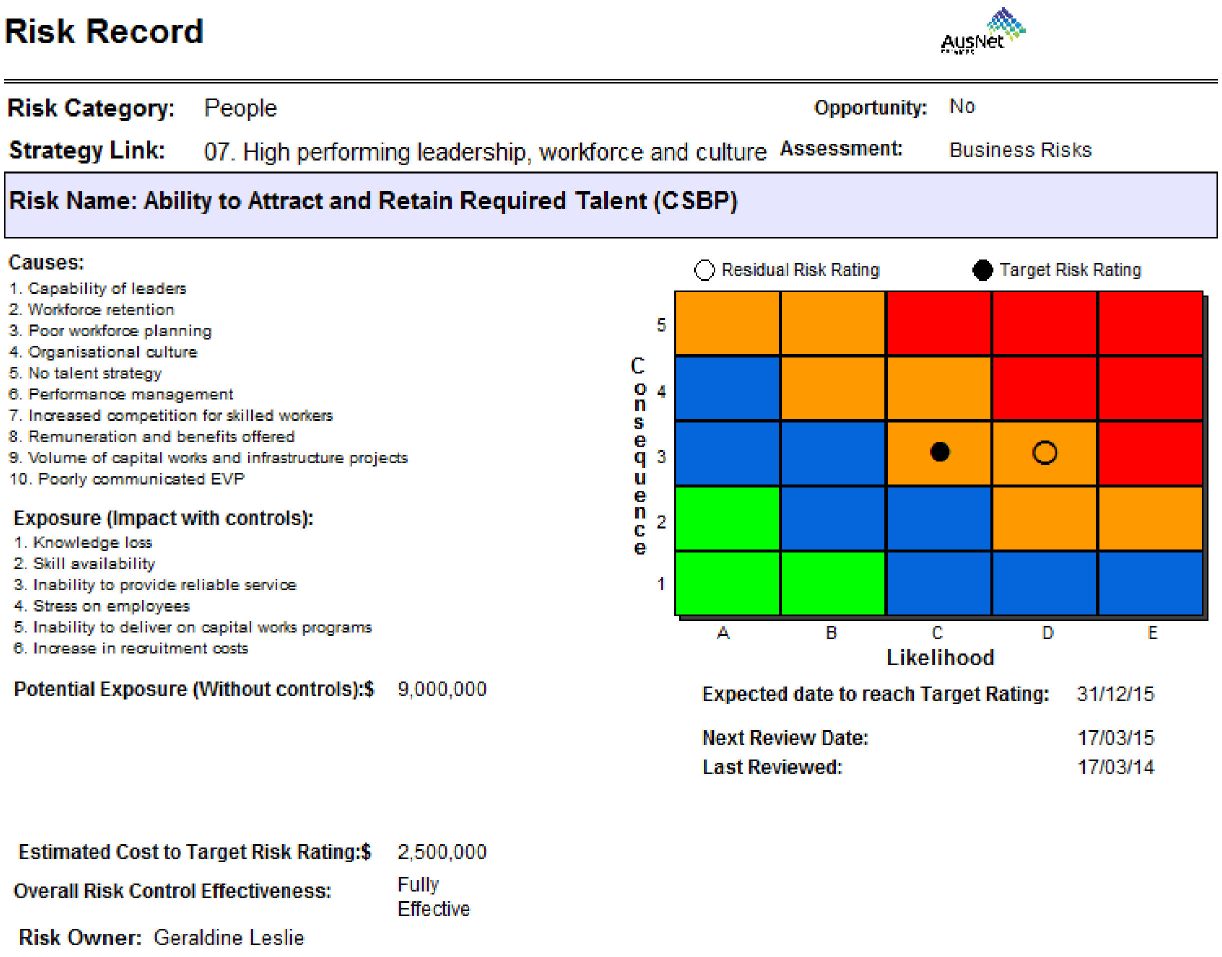
- **CURA excels at:**
  - ➢ Tracking control measures for risks.
  - ➢ Maintaining a workflow of control tasks.
  - ➢ Reporting of the general risk structure within the organisation and specific risk information.
  - ➢ Generally maintaining a central location of risk information.
  - ➢ Control self assessment.

Compliance Management

- **CARS is used to capture, maintain and report on obligations managed throughout the business.**

- **CARS excels at:**
  - ➢ Generally maintaining a central location of obligation information.
  - ➢ Tracking control measures for obligations.
  - ➢ Obligation self assessment.

Example Risk Record



Risk Record

Risk Category: People

Opportunity: No

Strategy Link: 07. High performing leadership, workforce and culture

Assessment: Business Risks

Risk Name: Ability to Attract and Retain Required Talent (CSBP)

Causes:

1. Capability of leaders
2. Workforce retention
3. Poor workforce planning
4. Organisational culture
5. No talent strategy
6. Performance management
7. Increased competition for skilled workers
8. Remuneration and benefits offered
9. Volume of capital works and infrastructure projects
10. Poorly communicated EVP

Exposure (Impact with controls):

1. Knowledge loss
2. Skill availability
3. Inability to provide reliable service
4. Stress on employees
5. Inability to deliver on capital works programs
6. Increase in recruitment costs

Potential Exposure (Without controls):$ 9,000,000

○ Residual Risk Rating ● Target Risk Rating

Consequence	A	B	C	D	E
5	🟧	🟧	🟥	🟥	🟥
4	🟦	🟧	🟧	🟥	🟥
3	🟦	🟦	🟧 ●	🟧 ○	🟥
2	🟩	🟦	🟦	🟧	🟧
1	🟩	🟩	🟦	🟦	🟦

Likelihood

Expected date to reach Target Rating: 31/12/15

Next Review Date: 17/03/15

Last Reviewed: 17/03/14

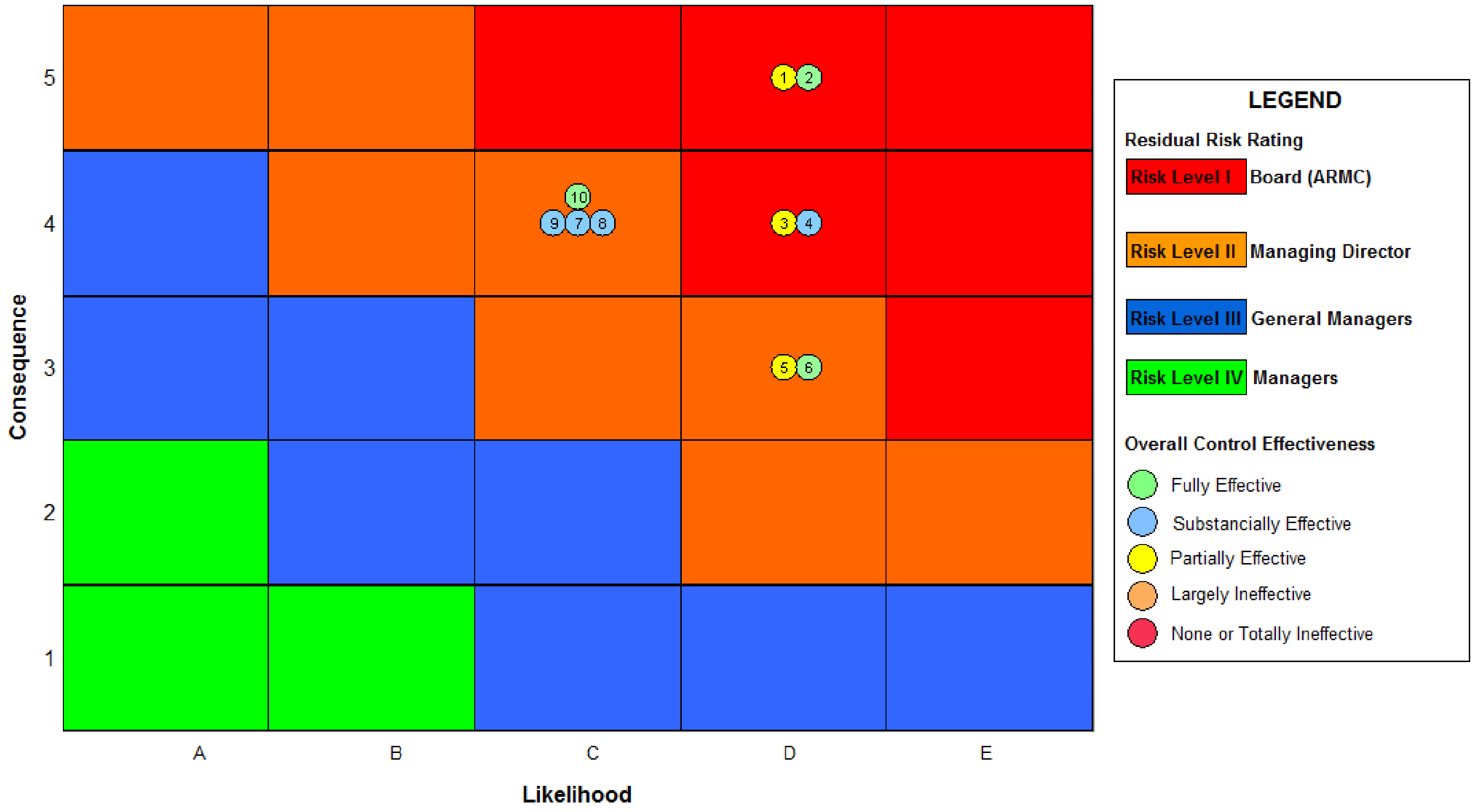
Estimated Cost to Target Risk Rating:$ 2,500,000

Overall Risk Control Effectiveness: Fully Effective

Risk Owner: Geraldine Leslie

Example Risk Register

Corporate Risk Profile - Top 10



Questions?