Overview of Risk & Compliance Management
for the Australian Energy Regulator (AER)

Elaine Carlin, Risk & Assurance
30 April 2015
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:

Key reference documents:
- Risk Management Framework (2013)
- Risk Management Guide (2009 – currently under revision)
- 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

Group Risk Committee (Executive leadership chaired by Managing Director)

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

General Managers (Risk ownership of enterprise level risks)

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

Risk Management

General Management

Finance

General Counsel & Co Sec

People, Safety & Customer

Select Solutions

Program, Strategy & Business Development

Service Delivery

ICT

AMI Program

Project Edison

Asset 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 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.

<table>
<thead>
<tr>
<th>Rating</th>
<th>Health, Safety and People</th>
<th>Environment &amp; Community</th>
<th>Reputation</th>
<th>Customers</th>
<th>Regulation, Legal and Compliance</th>
<th>Projects</th>
<th>Financial Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Multiple fatalities and/or Significant irreversible exposure to a health risk that affects greater than 10 people Wide-scale employee disengagement across the company Serious failings</td>
<td>Catastrophic long term environmental harm off-site and/or irreversible impact to cultural heritage area Community outrage potential large-scale class action</td>
<td>Critical event that the organisation could be forced to undergo significant change. Sustained adverse international national press reporting over several weeks Total loss of shareholder support who act to divest Reputation impacted with majority of stakeholders Licences to operate threatened</td>
<td>Loss of supply &gt;100 system minutes US$1M (electricity) or &gt;200,000 customers (gas) or System failure or Loss of supply to entire CBD</td>
<td>Major litigation or prosecution with damages of $50m+ plus significant costs Custodial sentence for company Executive Prolonged closure of operations by authorities Regulator conducts business through directives and suspended ability to operate</td>
<td>Corporate Business Plan objectives will be severely impaired by project failure</td>
<td>$100m+ loss or gain</td>
</tr>
<tr>
<td>4</td>
<td>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</td>
<td>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</td>
<td>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</td>
<td>Loss of supply &gt;30 system minutes US$1M (electricity) or &gt;100,000 customers (gas)</td>
<td>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</td>
<td>Major impact on the business objectives or significant impact on the project: - If the risk eventuates, 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</td>
<td>$10m - $99m loss or gain</td>
</tr>
</tbody>
</table>
## Consequence Criteria

<table>
<thead>
<tr>
<th>Rating</th>
<th>Health, Safety and People</th>
<th>Environment &amp; Community</th>
<th>Reputation</th>
<th>Customers</th>
<th>Regulation, Legal and Compliance</th>
<th>Projects</th>
<th>Financial Impact (AUS)</th>
</tr>
</thead>
</table>
| 3      | Serious injury            | Major event leading to location and off-site impact on ecology or damage to area of cultural heritage | Major event that causes adverse local press reporting over several days | Loss of supply >10 system minutes/USAID (electricity) or >5,000 customers (gas) | Major breach of law with punitive fine | Moderate impact on the business objectives or on the project:  
- Will cause major re-plan 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 costs | $1m – $5m loss or gain |
|        | Moderate permanent effects from injury or exposure. For example, serious burns, serious internal and/or head injuries, gassings that require hospitalisation | Medium term recovery | High potential for complaints from interested parties | | | |
|        | Significant employee disengagement or failures in non-critical areas | | | | | |
| 2      | Significant injury        | Medium term recovery, immaterial effect on environment or community required to return to pre-event conditions (e.g. noise, dust, odour) | Adverse local press reporting | Loss of supply >3 system minutes/USAID (electricity) or >500 customers (gas) | | Minor impact on the business objectives or on the project:  
- Inability to partly 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 – $500k loss or gain |
|        | 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 | | | | | |
| 1      | Minor injury              | Small, unconfined event, no impact on ecology or area of cultural heritage | No press reporting or external interest | Loss of supply >1 system minutes/USAID (electricity) or >100 customers (gas) | Minor legal issues, non-compliance and statutory fine  
Routine regulatory reporting and audits | | < $50k loss or gain |
|        | No medical treatment. For example, cuts, bruises, no measurable physical effects | Short term transient environmental or community impact: little action required | | | | |
|        | Short term loss of morale in non-critical areas | | | | | |

24 April 2015  
Elaine Carlin, Risk & Assurance
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.

<table>
<thead>
<tr>
<th>Rating</th>
<th>Criteria</th>
</tr>
</thead>
</table>
| 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.

<table>
<thead>
<tr>
<th>RCE</th>
<th>Guide</th>
<th>Indicators</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Fully Effective</strong></td>
<td>Nothing more to be done except review and monitor the existing controls</td>
<td>The control is:</td>
</tr>
<tr>
<td></td>
<td>Controls are well designed for the risk, address the root causes and</td>
<td>• Designed appropriately to meet its objectives</td>
</tr>
<tr>
<td></td>
<td>management believes that they are <strong>effective</strong> and reliable at all times.</td>
<td>• Operating as anticipated at all times</td>
</tr>
<tr>
<td></td>
<td>Control is deemed to be operational in excess of 95% of the time</td>
<td>• Documented and accessible</td>
</tr>
<tr>
<td><strong>Substantially Effective</strong></td>
<td>Most controls are designed correctly and are in place and effective. Some extra work to be done to improve operating effectiveness.</td>
<td>The control is:</td>
</tr>
<tr>
<td></td>
<td>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</td>
<td>• Designed appropriately to meet the majority of objectives</td>
</tr>
<tr>
<td></td>
<td>Control is deemed to be operational between 75% and 94% of the time</td>
<td>• Operating as anticipated some of the time</td>
</tr>
<tr>
<td><strong>Partially Effective</strong></td>
<td>Significant control gaps. Either controls do not treat root causes or they do not operate at all effectively.</td>
<td>The control is:</td>
</tr>
<tr>
<td></td>
<td>Control is deemed to be operational between 25% and 49% of the time</td>
<td>• Documented and accessible</td>
</tr>
<tr>
<td><strong>Largely Ineffective</strong></td>
<td>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.</td>
<td>The control is:</td>
</tr>
<tr>
<td></td>
<td>Alternatively, the risk is new and controls are yet to be implemented.</td>
<td>• Not designed appropriately to meet the majority of objectives</td>
</tr>
<tr>
<td></td>
<td>If any control exists it would be operational less than 25% of the time</td>
<td>• Not operating as anticipated at any time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not documented or accessible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not communicated and understood by relevant persons</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not reviewed on a regular basis (at least annually) or updated when necessary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not approved by the relevant Committee</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reviewed as part of the IA process and high rated issues were identified or not reviewed as part of the IA</td>
</tr>
<tr>
<td><strong>None or totally ineffective</strong></td>
<td>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.</td>
<td>The control is:</td>
</tr>
<tr>
<td></td>
<td>Alternatively, the risk is new and controls are yet to be implemented.</td>
<td>• Not designed appropriately to meet its objectives</td>
</tr>
<tr>
<td></td>
<td>If any control exists it would be operational less than 25% of the time</td>
<td>• Not operating as anticipated at any time</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not documented or accessible</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not communicated and understood by relevant persons</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not reviewed on a regular basis (at least annually) or updated when necessary</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Not approved by the relevant Committee</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Reviewed as part of the IA process and high rated issues were identified or not in existence</td>
</tr>
</tbody>
</table>
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.
The matrix should be used to determine the priority of attention to the risk. 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.

<table>
<thead>
<tr>
<th>Residual risk level</th>
<th>Suggested action</th>
<th>Suggested timing</th>
<th>Authority for continued toleration of residual risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>Take immediate action to treat risk.</td>
<td>Short term. Action Plans prepared and normally implemented within 1 month.</td>
<td>Board (ARMC)</td>
</tr>
<tr>
<td>II</td>
<td>Plan to deal with in keeping with the business plan.</td>
<td>Medium term. Action Plans prepared and normally implemented within 6 months.</td>
<td>Managing Director</td>
</tr>
<tr>
<td>III</td>
<td>Plan in keeping with all other priorities.</td>
<td>Action Plans prepared and normally implemented within 1 year</td>
<td>General Managers</td>
</tr>
<tr>
<td>IV</td>
<td>Will still require attention within existing operations.</td>
<td>Ongoing control as part of a management system.</td>
<td>Managers</td>
</tr>
</tbody>
</table>
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.
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
Strategy Link: 07. High performing leadership, workforce and culture
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 services
4. Stress on employees
5. Inability to deliver on capital works programs
6. Increase in recruitment costs

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

Estimated Cost to Target Risk Rating: $2,500,000
Overall Risk Control Effectiveness: Fully Effective

Risk Owner: Geraldine Leslie

Expected date to reach Target Rating: 31/12/15
Next Review Date: 17/03/15
Last Reviewed: 17/03/14
Questions?