



Australian Association of Agricultural Consultants

Operational Risk Management

May 2010



Why is Operational Risk Management Important?

- Managing risk has always been an inherent part of running our business
- Operational Risk has gained a bigger profile during the past decade, due to increasing loss events and regulatory requirements
- We all want to do the best for our business
- Understanding what risks you face, how big they are and how likely they are to occur, helps to inform your decision making
- To ensure there are 'No Surprises' that affect the bottom line
- Infrastructure spend needs to balance risk and return
- Consequences of failing to manage Operational Risk can include Financial losses, disruption to the business processes, increased Regulatory scrutiny, Reputational and Customer impacts and Management Remediation (time impost).



What is Operational Risk?

Risk

Is the possibility of a future negative outcome; events or conditions that may occur, and whose occurrence, if it does take place, has a harmful or negative effect.

Operational Risk

Is the risk involved with running a business. Operational risk represents some of the key risks to the business world today. It exists throughout all of our businesses at all levels and is represented in most activities we undertake.

Operational risk is the risk of loss resulting from inadequate or failed internal processes, people and systems or external events



Types of Operational Risk facing Businesses



Operational Risk Framework - Overview

- The Operational Risk Framework (ORF) outlines the core Operational Risk Principles for identifying, assessing, managing, monitoring and reporting on operational risks.
- Risk Event Types and Control Categories have been established which prompt the consistent consideration and classification of operational risks and operational risk events, including Fraud, People, Processing and Business Interruption Risks.
- The ORF is supported by a number of core operational risk processes which include the Group Integrated Risk Profiling Process (IRP) and Group Event Management Process. The IRP outlines the approach to considering risks emanating from Change Initiatives.
- Change Initiatives (e.g. New Products, Outsourcing, etc) are subject to the various Risk Change Processes in place across the Group.
- The delivered risks associated with Change Initiatives are incorporated into the Business Unit Risk Profiles and treated as one of the core inputs. This includes risks associated with Products.



Operational Risk Framework - Principals

- Business objectives must be captured & understood to ensure that operational risks to the achievement of those objectives can be identified and assessed;
- Business Management must adopt an open & honest approach to operational risk identification;
- Risk & Event impacts must be assessed based on financial & non-financial impacts, taking into consideration the effectiveness of controls;
- Business Management must own the operation of controls & ensure that those controls are being effectively performed & monitored;
- Key Risk Indicators must be defined & adopted around risks & the performance of controls. Must be used to monitor the overall operational risk profile
- Regular reports must be provided to Regional Risk Committees



Operational Risk Framework - Outcomes

Effective implementation and use will lead to:

- Consistency in the identification, assessment, mitigation, monitoring and reporting of Operational Risk
- Proactive identification and management of Operational Risks and events to minimise:
 - financial losses
 - disruption to business processes
 - non-financial impacts including regulatory, reputation and customer impacts
- All staff taking responsibility and ownership for managing the Operational Risk inherent in their day-to-day activities
- Risk-reward decisions being made on an informed basis to improve Operational Risk awareness or acceptance of Operational Risks
- Promoting and embedding a risk conscious culture and behaviour throughout the Group



Operational Risk Profiling - Key Questions

<p>Business Environment</p>	<ul style="list-style-type: none"> ▪ What are the key business objectives? ▪ What are the products and services offered to your customers? ▪ What changes are planned for your business? e.g. restructure, relocation, new systems?
<p>Risk Identification</p>	<ul style="list-style-type: none"> ▪ What risks/uncertainties face your business? ▪ Are you confident that these are all the risks that your business faces? ▪ Have you drawn on the opinion and experience of your business unit's management and those who interact with it, e.g. Finance partners, Technology partners, in identifying risks? ▪ Have you identified risks with potential Extreme Impacts?
<p>Risk Assessment</p>	<ul style="list-style-type: none"> ▪ How do you determine the impact on your business objectives of your customers' experience? ▪ Do you know how well you mitigate those risks and the effectiveness of your controls? ▪ Do you understand the potential financial and non-financial impacts of your risks?
<p>Risk Mitigation</p>	<ul style="list-style-type: none"> ▪ What other performance or other management information do you use to monitor business performance & associated risks? ▪ Do you intend to improve the control environment or accept a certain level of risk based on this information? Alternatively, would you consider transferring the risks identified? ▪ Are you willing to accept risk & control weaknesses, transfer to another provider or mitigate through management actions?
<p>Risk Reporting</p>	<ul style="list-style-type: none"> ▪ How do you discuss, share information & escalate risks within your business? ▪ Who needs to know and when?

