Your Risk Framework Design

RiskNZ Conference

‘Seize the Day’- – Stepping forward in challenging times
23 & 24 October 2014
Te Papa Wellington

Speaker: Helen Marsden

Introductions

Helen Marsden – Executive MBA

Risk Management Experience

- Currently Risk Manager at Unison Networks Limited
- 3 years consulting for PwC on Governance, Risk and Compliance across a number of industries
- 5 years as a Senior Operational Risk Manager driving Regulator (RBNZ and APRA) approved and accredited operational risk framework and risk methodologies across Westpac New Zealand
- 3 years Operational and Compliance Risk Manager embedded in Business Units for ANZ Bank and UDC Finance

Presentation Overview

- ✓ Objectives of Risk Management
- ✓ Regulated and / or structured risk frameworks, should your organisations risk processes use a similar benchmark?
- ✓ What does a successful risk management programme look like? (Risk challenge: measuring what doesn’t go wrong?)
- ✓ What are the factors to consider when tailoring a framework for your organisation?
- ✓ Case study – how Risk Management can go wrong if not completely aligned to the function of the organisation
- ✓ How to phase implementation of a successful Risk Management Programme

Objective of Risk Management

- **Risk**: minimise the surprise factor and effects of uncertainty on the achievement of strategic objectives, while maximising opportunities and an entrepreneurial environment
- **Governance:** provides senior leaders with key information that provides positive assurance to the Board that risks for delivering on strategy are managed within appetite
- **Compliance:** develop and implement risk and regulatory compliance mitigation plans assigned to one owner

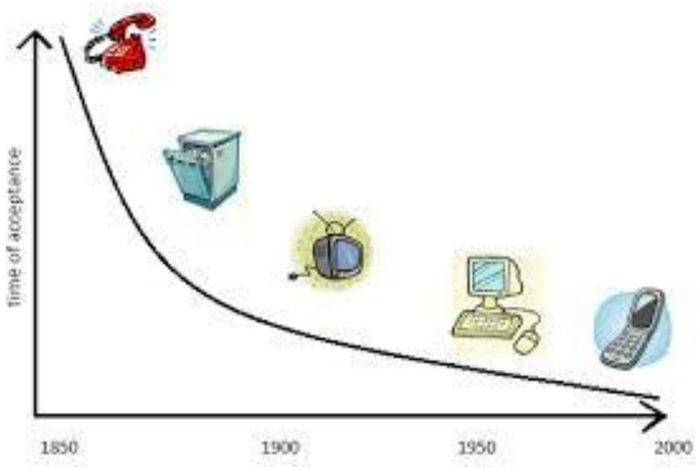
Answer to Risk Management….. Buy Insurance – Right?

Yeah Right….What about liquidity

Why Bother

- Greater global integration therefore impacted by global trends e.g. financial crisis
- Business specialisation / integration e.g. supply chain
- Arguably compared to prior decades one constant today is exponential growth in the rate of change
  - Organisations have responded by:
    - ✓ Being adaptable and responsive
    - ✓ Being innovative
    - ✓ Empowering staff

❖ With empowerment, innovation and adaptability EVERYONE must take responsibility for risk



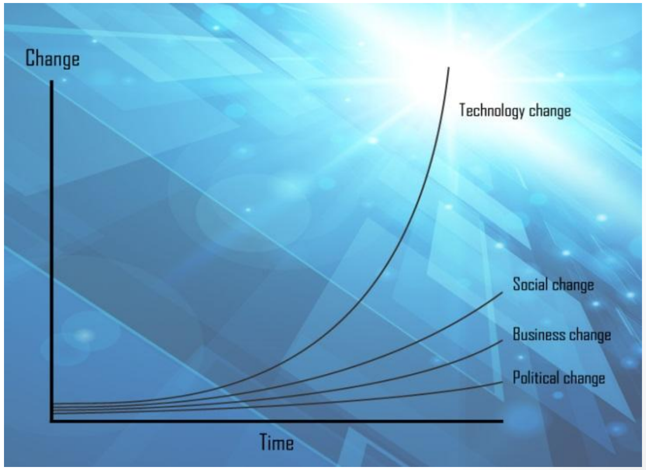


Figure: *Rate of technology change and the shrinking time of acceptance.* Adapted from (Henriques, 2001)

Designing Your Risk Framework

There are a number of risk management standards that are designed to help with development and implementation of a successful risk process e.g.

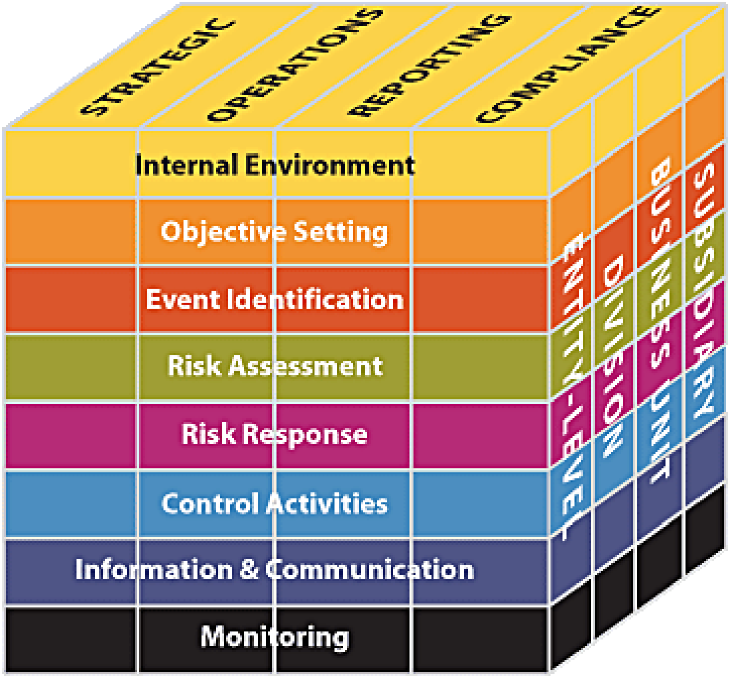
- COSO's ERM – *Integrated Framework*
- ISO 31000 – *Risk Management Standard*
- Federation of European Risk Management Associations (FERMA) – *Risk Management Standard based on 2002 UK standard*
- Basel Committee International Banking Regulations – *Operational Risk Regulations and three lines of defence*

- Unless your organisation is subject to risk regulations utilise standards to support and drive a successful programme

- Refresh to maintain a 'fit for purpose' framework especially if the organisations environment changes e.g. regulatory landscape

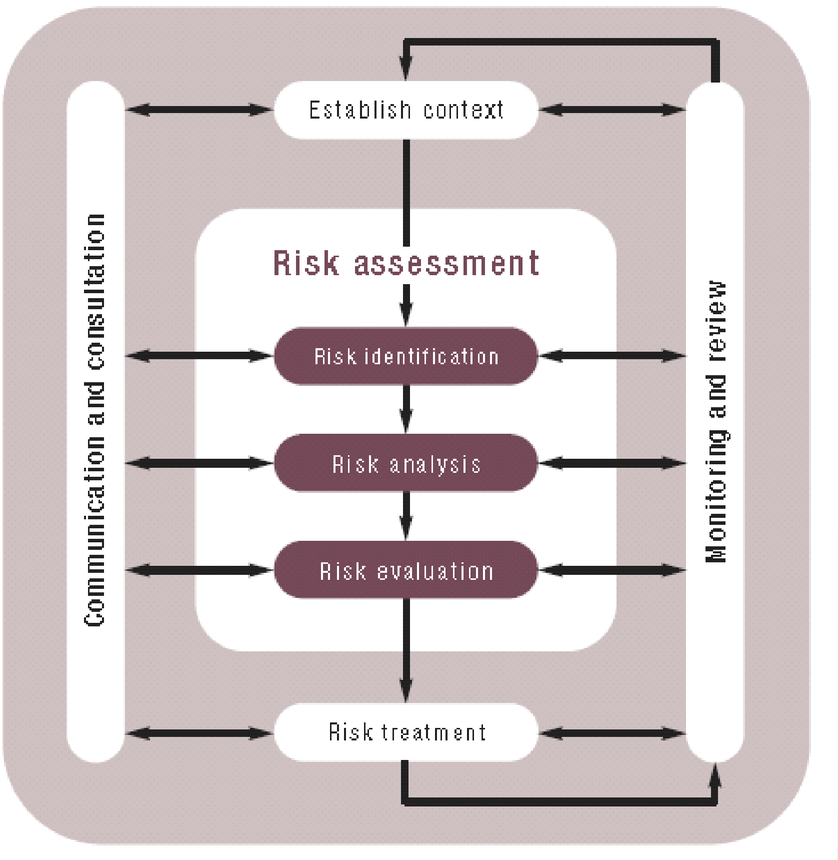
Example - Standards Detailed

- COSO –developed the ERM Integrated Framework (2004), aka the COSO Cube, an update to the initial COSO I framework (1992)



Example - Standards Detailed

- ISO 31000:2009 provides generic guidelines for the design, implementation and maintenance of risk management processes across the organisation.
- This enable all strategic, management and operational tasks in projects, functions and processes to be aligned to a common set of risk management objectives.



Basel Operational Risk Standard

- Basel II issued by the Basel Committee on Banking Supervision in June 2004, provided international standards for banking regulators to control Banks' capital requirements aimed to minimise financial collapse during significant events.

- The Accord defines operational risk as 'The risk of loss arising from inadequate or failed internal processes, people or systems, or from external events'. Therefore considering the impact of both the internal and external environment.

- Many Banks responded by progressing sophisticated frameworks that included lines of defence and scenario analysis.

Organisational Considerations When Tailoring A Framework

When tailoring a framework if necessary cherry-pick ‘fit for purpose’ aspect from prescribed standards and consider:

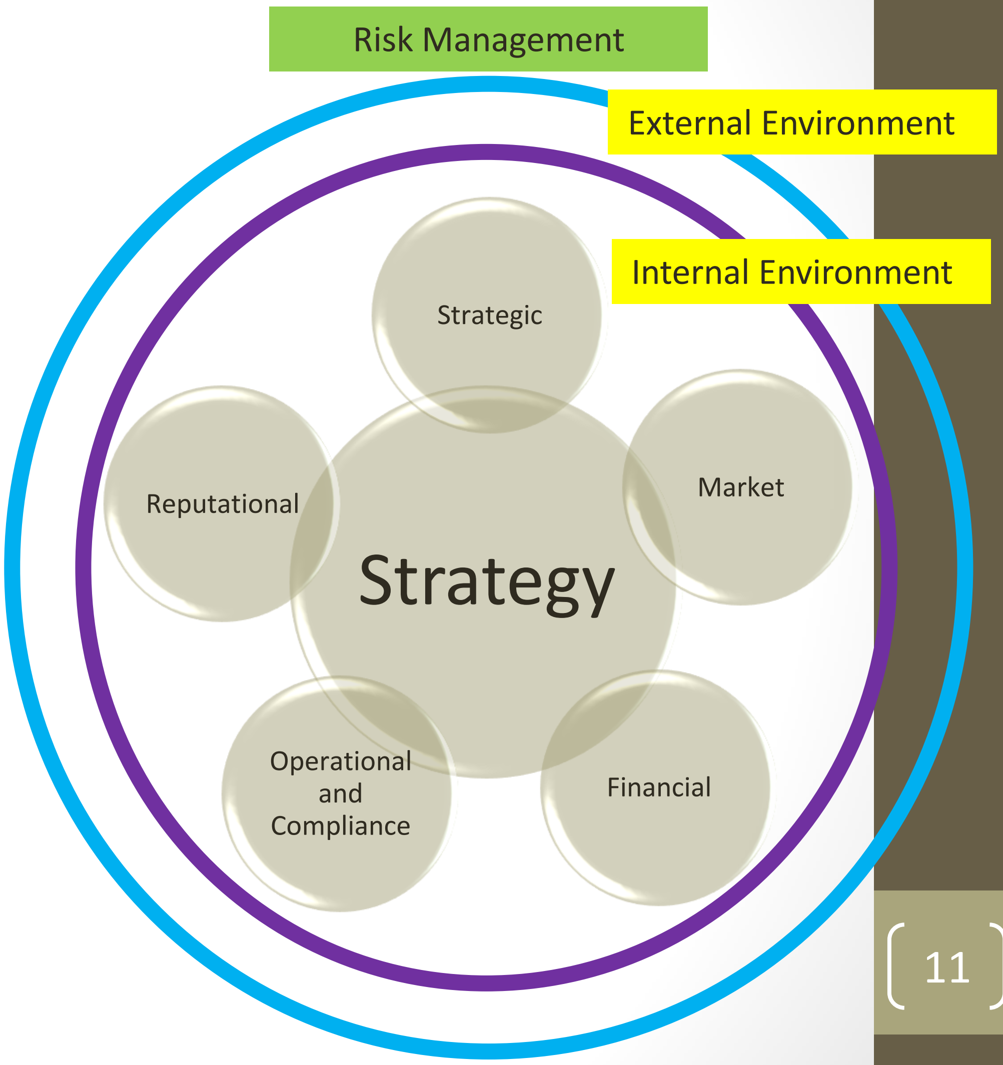
- Required Governance Structure
  - <u>Size</u> and scale of the organisation
  - <u>Complexity</u> of the organisations structure
  - <u>Appetite</u> (risk-takers v risk adverse)
- Monitoring and oversight (degree of disaggregation)
  - Complexity of the organisation <u>business model</u>
  - <u>Innovative</u> nature of the business and rates of change
  - <u>Alignment</u> or diversity of the organisation
- Levels of structure processes
  - Level of true staff <u>empowerment</u>
  - Organisational <u>values</u>

A Successful Risk Programme

- Focusses on the successful achievement of objectives across all levels of the organisation continuing to reference against the internal and external environment

- ISO 31000 – places strategic objectives at the centre of risk management changing the definition of risk from 'probability of loss' to 'effect on objectives'

- Enterprise focussed and considers impact across all risk classes equally



A Successful Risk Programme

Done effectively risk management helps an organisation:

- Deliver on our strategy by:
  - maximising efficiencies through internal change while,
  - minimising costly surprises, and
  - identifying and capturing external opportunities in an ever changing world.
- Providing an enterprise-wide lens for:
  - improving strategic decision making, and
  - cutting through business silos and risk categories silos (financial, market, operational) to attain one view.

The following attributes are evident in a successfully tailored and implemented programme:

- Open communication and challenge at all levels
- Broader team involvement , including a view of risk aggregation across silos
- Culture that is engaged and committed
- Candid and honest conversation without fear of retribution
- Executive engagement with time commitment from all staff (tone from the top)
- A ‘fit for purpose’ governance structure

An Incomplete Risk Programme

- Removed from strategy and objectives
- No structure or formal framework
- No consistency in application across the organisation
- No common language
- Lack of involvement of stakeholders
- Little involvement from Senior Executives
- Compliance driven and bureaucratic tick box exercise
- Added complexity
- Removed from reality
- No plan or vision for risk management
- No coordination or oversight
- Siloes across the business and across risk classes

Implementing Your Framework

Significant commitment to develop and implement (short-term)

- Workshop in two phases:
  1. Risk identification (e.g. Bowtie Analysis)
  2. Control identification (part two of the bowtie) and assessment

Not a one off project, risk maturity takes time, so plan, prioritise and be patient

- Questions