Implementing ISO 31000 …but how do you do it?

Grant Purdy
Associate Director, Broadleaf Capital International
Chair, Standards Australia and New Zealand Risk Management Committee
Nominated Expert - ISO WG on Risk Management

The Pivotal Definition

Risk

effect of uncertainty on objectives

NOTE 1 An effect may be positive, negative, or a deviation from the expected.
NOTE 2 An objective may be financial, related to health and safety, or defined in other terms.
NOTE 3 Risk is often described by an event, a change in circumstances, a consequence, or a combination of these and how they may affect the achievement of objectives.
NOTE 4 Risk can be expressed in terms of a combination of the consequences of an event or a change in circumstances, and their likelihood.

Is this a car?

Spot the difference? Between this....
Risk Management Components - The (often missing) organisational context

- Commit and Mandate
- Designing the Framework
- Mandate and commitment
- Continual improvement of the framework
- Implementing risk management
- Monitoring and reviewing the framework
- Establish the context
- Identify risks
- Analyse risks
- Evaluate risks
- Treat risks
- RM Information System
- Risk Registers
- Treatment Plan
- Assurance Plan
- Reporting templates

ISO 31000 Framework for Risk Management

Clause 6

Simple summary

“it ain't what you do …
It's the way that you do it”
Principles (Clause 4) - risk management should:

1. Create value
2. An integral part of organisational processes
3. Part of decision making
4. Explicitly address uncertainty
5. Be systematic and structured
6. Be based on the best available information
7. Be tailored
8. Take into account human factors
9. Be transparent and inclusive
10. Be dynamic, iterative and responsive to change
11. Be capable of continual improvement and enhancement

Annex A - Attributes of excellence in risk management

1. A pronounced emphasis on continuous improvement
2. Comprehensive, fully defined and fully accepted accountability for risks, controls and treatment tasks.
3. All decision making within the organization involves the explicit consideration of risks and the application of the risk management process to some appropriate degree.
4. Continual communications and highly visible, comprehensive and frequent reporting.
5. Risk management is always viewed as a core organizational process.

So how do you start? 1 - the “cunning plan”

1. Conduct a gap analysis – take stock
2. Set a realistic timetable (years)
3. Get a budget
4. Get some help
5. Bleed in the processes (one a year?)
6. Decide when you will be ready to roll (down)
7. Decide on the ‘early adopters’ with credibility and start with them
8. Decide on the ‘blockers’ and take them on later
9. Look out for opportunity to ‘showcase’

So how do you start? 2 - receiving the blessing

1. Get a sponsor (CEO/CFO/Co Sec)
2. Write a motivational policy statement and get the CEO to own it and sign
3. Tell the risk/audit committee or Board what you are doing and when you will report to them on progress
4. Set up a W/G with all departments involved – especially the ‘difficult ones’
5. Get consultation going on Standards and Guidelines
6. Agree a timetable for engagement of each department/chunk
7. Get Champions nominated
8. Make friends with the Internal Auditors

So how do you start? 3 - tricks of the trade

• Don’t do a pilot study or call it an initiative
• Set ‘Standards’ and write Guidelines (not Policy and Procedures manuals!!)
• Don’t outsource it
• Don’t try to force people to do it – you need to make your case
• Don’t ever do it for them – after the first time
• Don’t start until you’re ready
• Never agree to just do it “for reporting purposes”
• Don’t over simplify (simple = yes, simplistic = no)
• Don’t start at the bottom of the organisation

Roll down or Roll-up?

• Answer – both!
• You roll-down risk management, getting buy-in and ownership
• You roll-up risk profiles to produce consolidated profiles
The roll-down

1. "Engage" the management team at that level
   - Change their vocabulary and make your case
   - Get them to discuss what they perceive as the major risks — and compare across the team!
2. Facilitate a self-evaluation of their current approaches to risk management using a structured maturity evaluation
3. Facilitate a strategic risk assessment — what are those things that might prevent or enhance us achieving our strategic objectives

Risk Management Maturity Measurement System

<table>
<thead>
<tr>
<th>Maturity</th>
<th>None</th>
<th>Very Little</th>
<th>Some</th>
<th>Good</th>
<th>Complete</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat</td>
<td>0</td>
<td>1</td>
<td>5</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Practice</td>
<td>0</td>
<td>3</td>
<td>7</td>
<td>15</td>
<td>20</td>
</tr>
</tbody>
</table>

Evaluation Protocol - for example

Maturity evaluation
- Compare the current year to the past – ‘footprinting’
- Generate a numerical score that links to KPIs and performance management
- Link to insurance premium distribution and create an incentive
- Validate through Internal Audit – it gives them a protocol to follow
- Refocus on what matters for your organisation
- Raise the bar after a few years

The RMIS manages the outputs

Baseline Risk Assessment
- Risk Register
  - Risks
  - Causes
  - Controls
  - Risk ratings etc.
  - Risk owners
  - Control owners
- Risk Treatment Plan
  - Tasks
  - Task owners
  - Timelines
  - Budgets?

Maturity Evaluation
- Risk Management Plan
  - Tasks
    - For embedding
    - For rolling out further
    - Training
  - Special risk treatment (eg BCP)
  - Measurement
  - KPIs
  - Task owners
  - Timelines

Conclusions
1. ISO 31000 Risk Management is not just about risk assessment for reporting
2. It is a continuous process that ‘infects’ an organisation
3. It will not happen by accident
4. It should be carefully planned, managed and resourced
5. The benefits (in time) are remarkable and valuable
Uncertainty is the human paradox:
we fear it, but we need it!