Presenter: Ian Musweu
FCCA, FZICA, CRA

Head of Risk and Assurance Professional Insurance
Contents:

• Introduction;
• Overview of the two major frameworks
• Frameworks side by side Similarities and differences
• Pros and Cons of the frameworks
• Conclusion and new developments
Introduction:

King III report recognizes the role of the Board and governance in as far as risk management is concerned. There is emphasis on the need for a risk management structure in the governance of an organization. Many approaches are identified which include but are not limited to: COSO, ISO, IRMSA, ERM Code of Practice, IRM (UK)
Background of ISO 31000

• “Risk Management – Principles and Guidelines” is the title of the international standard on the practice of risk management. Also known as ISO 31000:2009, it was published in November of 2009. The standard was created by a working group that included technical advisors from 18 countries. In a series of six meetings over several years, the group revised the Australia/New Zealand risk management standard (AS/NZS 4360:2004) to create a standard that can be used by a wide variety of organizations in any country for any type of operation, regardless of complexity, size or type.
Foundation of ISO 31000

• The basis for ISO 31000 follows this trajectory:
  1. All organizations exist to achieve their objectives;
  2. Many internal and external factors affect those objectives, causing uncertainty about whether the organization will achieve its objectives;
  3. The effect this uncertainty has on an organization’s objectives is “risk.”

• Hence the standard emphasizes the need for the linking of key risks and the risk management process to an organization’s strategic objectives.

• Need to identify risks beyond insurable or industrial safety risks (including strategic, reputational and financial risks) as well as assigning responsibility for risk management across the entire organization (risk ownership).
**Principles for managing risk (Clause 3)**

1. Creates value
2. Integral part of organisational processes
3. Part of decision making
4. Explicitly addresses uncertainty
5. Systematic, structured & timely
6. Based on the best available information
7. Tailored
8. Takes human & cultural factors into account
9. Transparent & inclusive
10. Dynamic, iterative & responsive to change
11. Facilitates continual improvement & enhancement of the organisation

**Framework for managing risk (Clause 4)**

- Mandate & commitment
- Design of framework for managing risk
- Continual improvement of the framework
- Implementing risk management
- Monitoring & review of the framework

**Process for managing risk (Clause 5)**

- Establishing the Context
- Risk Assessment
- Risk Identification
- Risk Analysis
- Risk Evaluation
- Risk Treatment

**Attributes of enhanced risk management (Annex A - Informative)**

- AS4360 – Covered partially in Section 4 “Establishing effective risk management”
- AS4360 – Fully covered in Section 3 “Risk Management Process”
- AS4360 – Not covered
In 2001, COSO initiated a project, and engaged Price waterhouse Coopers, to develop a framework that would be readily usable by managements to evaluate and improve their organizations’ enterprise risk management.

The COSO ERM framework consists of eight interrelated components derived from COSO conception of how management both runs an organization and integrates risk management into its other management processes.
Eight components of COSO ERM

- Internal environment (i.e., the organizational risk culture);
- Objective setting (i.e., the organization's objectives);
- Event identification (i.e., the events that might affect objectives);
- Risk assessment (i.e., how risks are assessed);
- Risk response (i.e., how risks are managed);
- Control activities (i.e., the policies and procedures ensuring that risk responses are carried out);
- Information and communication (i.e., how risk information is communicated); and
- Monitoring (i.e., how ERM as a whole is performing and whether it needs improvement).
The two frameworks side by side

<table>
<thead>
<tr>
<th>Key term/ description</th>
<th>ISO 31000</th>
<th>COSO II/ COSO ERM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>This International Standard provides principles and generic guidelines on risk management… it can be used by any public, private or community enterprise, association, group or individual. Therefore, this International Standard is not specific to any industry or sector.</td>
<td>This definition of ERM is purposefully broad. It captures key concepts fundamental to how companies and other organizations manage risk, providing a basis for application across organizations, industries and sectors. It focuses directly on achievement of objectives established by a particular entity and provides a basis for defining enterprise risk management effectiveness.</td>
</tr>
<tr>
<td>Risk management, defined.</td>
<td>Coordinated activities to direct and control an organization with regard to risk.</td>
<td>Enterprise risk management is a process, effected by an entity’s board of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risk to be within its risk appetite, to provide reasonable assurance regarding the achievement of entity objectives.</td>
</tr>
<tr>
<td>Key term/ description</td>
<td>ISO 31000</td>
<td>COSO II/ COSO ERM</td>
</tr>
<tr>
<td>------------------------</td>
<td>-----------</td>
<td>--------------------</td>
</tr>
<tr>
<td>Risk, defined.</td>
<td>The effect of uncertainty upon objectives.</td>
<td>The possibility that an event will occur and adversely affect the achievement of objectives.</td>
</tr>
<tr>
<td>Risk appetite, defined.</td>
<td>The amount and type of risk that an organization is willing to pursue or retain.</td>
<td>A broad amount of risk an entity is willing to accept in pursuit of its mission or vision.</td>
</tr>
<tr>
<td>Risk assessment defined</td>
<td>The overall process of risk identification, risk analysis and risk evaluation.</td>
<td>Risks are analyzed considering likelihood and impact, as a basis for determining how they should be managed. Risk are assessed on an inherent and a residual basis.</td>
</tr>
</tbody>
</table>
| Risk Management process | Continually and interactively: Communicate and consult  
- Establish the context  
- Risk assessment:  
  - Identification  
  - Analysis  
  - Evaluation  
- Risk treatment Continually & iteratively: Monitor and review |  
- Internal environment  
- Objective setting  
- Event identification  
- Risk assessment  
- Risk response  
- Control activities  
- Info & communication  
- Monitoring |
### Pros and Cons for the two frameworks

<table>
<thead>
<tr>
<th>ISO 31000</th>
<th>COSO ERM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Easier to understand and explain to others. User friendly</td>
<td>It is comprehensive and has stood the test of time</td>
</tr>
<tr>
<td>A better ‘how to’ guide, easier to use when implementing risk management</td>
<td>It links to the COSO internal control framework</td>
</tr>
<tr>
<td>More focused on risk and less on audit and controls than COSO</td>
<td>It has a better discussion of risk appetite</td>
</tr>
<tr>
<td>Flexible, less prescriptive, easily tailored</td>
<td>It is stronger on corporate governance</td>
</tr>
</tbody>
</table>
Pros and Cons for the two frameworks

<table>
<thead>
<tr>
<th>ISO 31000</th>
<th>COSO ERM</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO 31000 is too high level</td>
<td>COSO ERM is too detailed and the cube is confusing</td>
</tr>
</tbody>
</table>
CONCLUSION

The frameworks have more things in common than different. Internal auditors may find it a lot easier to use the COSO II framework based on the background internal control framework however, the flexibility of ISO 31000 makes it very attractive to use for risk managers without audit background.

There is more inclination to comply with the COSO from organizations which have a USA background due to the growing need for compliance. In May 2013 there was a revision to the original COSO framework that may want to look at. October 2014 COSO announced the project to update the COSO II on ERM.