A conceptual framework on establishing a risk management framework within existing university assessment and evaluation practices

Fernando Padró
28 October, 2013
AHEEF Conference
Topics covered

- Background into ERM – issues of external and internal governance
- Issues regarding definitions
- COSO Cube
- ISO 31000
- Current projects at USQ regarding the introduction of ERM into unit decisionmaking
Enterprise Risk Management: A way to provide opportunity through identified capacity to accept or move to changing conditions

A risk is a chance you take; if it fails you can recover. A gamble is a chance taken; if it fails, recovery is impossible.

Erwin Rommel
TEQSA’s definition of regulatory risk ‘refers to actual or potential risk events (regarding a provider’s operations and performance) which indicate that the provider may not meet the Threshold Standards (either currently or in the future)’ (TEQSA, 2012, p. 34).
Other definitions of risk – How an institution defines and looks at risk is a key component on how to manage it!

- Risk is a function of likelihood and impact (Curtis & Carey, 2012).

- Risk is an uncertain future outcome that can either improve or worsen position (European Risk Management Association adopted the ISO/IEC Guide 73 (FERMA2002), which was superseded by ISO 31000).


- Risk and Insurance Management Society [RIMS] (2012): risk as an uncertain future outcome that can either improve or worsen position.

- Committee of Sponsoring Organizations of the Treadway Commission [COSO] (2013): risk as the possibility that an event will occur and adversely affect the achievement of objectives.

These different committees also have ancillary definitions pertaining to risk activities, tolerances, appetites, etc. that undergird these definitions and shape the practice of ERM under these models.
It’s about optimal risk taking (Curtis & Carey, 2012)
Improvement through control reconfiguration (COSO, 2007)
COSO Framework (COSO, 2013)
Original COSO cube (COSO, 2004)
Key elements of COSO framework COSO, 2004)

**Internal Environment**
- Risk Management Philosophy
- Risk Appetite
- Board of Directors
- Integrity and Ethical Values
- Commitment to Competence
- Organizational Structure
- Assignment of Authority and Responsibility
- Human Resource Standards

**Objective Setting**
- Strategic Objectives
- Related Objectives
- Selected Objectives
- Risk Appetite
- Risk Tolerances

**Event Identification**
- Events
- Influencing Factors
- Event Identification Techniques
- Event Interdependencies
- Event Categories
- Distinguishing Risks and Opportunities

**Risk Assessment**
- Inherent and Residual Risk
- Establishing Likelihood and Impact
- Data Sources
- Assessment Techniques
- Event Relationships

**Risk Response**
- Evaluating Possible Responses
- Selected Responses
- Portfolio View

**Control Activities**
- Integration with Risk Response
- Types of Control Activities
- Policies and Procedures
- Controls over Information Systems
- Entity Specific

**Information and Communication**
- Information
- Communication

**Monitoring**
- Ongoing Monitoring Activities
- Separate Evaluations
- Reporting Deficiencies
Information flow within ERM (COSO, 2004)
COSO monitoring process (COSO, 2007)
Update articulates principles of effective internal control

Control Environment
1. Demonstrates commitment to integrity and ethical values
2. Exercises oversight responsibility
3. Establishes structure, authority and responsibility
4. Demonstrates commitment to competence
5. Enforces accountability

Risk Assessment
6. Specifies suitable objectives
7. Identifies and analyzes risk
8. Assesses fraud risk
9. Identifies and analyzes significant change

Control Activities
10. Selects and develops control activities
11. Selects and develops general controls over technology
12. Deploys through policies and procedures

Information & Communication
13. Uses relevant information
14. Communicates internally
15. Communicates externally

Monitoring Activities
16. Conducts ongoing and/or separate evaluations
17. Evaluates and communicates deficiencies

source: COSO, May 2013
Developing risk appetite the COSO way (Rittenberg & Martens, 2012)

<table>
<thead>
<tr>
<th>Overview of Considerations Affecting Risk Appetite</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Existing Risk Profile</strong></td>
</tr>
<tr>
<td>The current level and distribution of risks across the entity and across various risk categories</td>
</tr>
<tr>
<td><strong>Risk Capacity</strong></td>
</tr>
<tr>
<td>The amount of risk that the entity is able to support in pursuit of its objectives</td>
</tr>
<tr>
<td><strong>Risk Tolerance</strong></td>
</tr>
<tr>
<td>Acceptable level of variation an entity is willing to accept regarding the pursuit of its objectives</td>
</tr>
<tr>
<td><strong>Attitudes Towards Risk</strong></td>
</tr>
<tr>
<td>The attitudes towards growth, risk, and return</td>
</tr>
</tbody>
</table>

**Determination of Risk Appetite**

---

*UNIVERSITY OF SOUTHERN QUEENSLAND*
How COSO sees inter-relationships (Rittenberg & Martens, 2012)

**Interrelationship of Strategy, Management Decisions, and Risk Appetite**

- Sets strategic goal and objectives
- Formulates strategies
  - Strategy 1
  - Strategy 2
  - Strategy 3
  - ...
- Establishes operations, compliance, and reporting objectives
- Makes decisions on how to manage risks relating to the achievement of objectives

Considers risk appetite in setting of strategies, objectives, and how to manage risks
How risk appetite controls process in COSO
(Rittenberg & Martens, 2012)
It’s about mapping opportunities as well as risks (Curtis & Carey, 2012)

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Opportunities</th>
<th>Impact</th>
<th>Risks</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Extreme</td>
<td>Incidental</td>
<td>Minor</td>
</tr>
<tr>
<td>Frequent</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rare</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
A decision continuum (Rittenberg & Martens, 2012)

- Acceptable
  - Increased costs due to incompatibility with legacy computer systems
- Not Acceptable
  - Reduced security of IT
  - Reduced teaching reputation
  - Reduced research reputation
ISO 31000 (ISO, 2009)

Figure 1 — Relationships between the risk management principles, framework, and process

Principles (Clause 3)

- a) Creates value
- b) Integral part of organizational processes
- c) Part of decision making
- d) Explicitly addresses uncertainty
- e) Systematic, structured and timely
- f) Based on the best available information
- g) Tailored
- h) Takes human and cultural factors into account
- i) Transparent and inclusive
- j) Dynamic, iterative and responsive to change
- k) Facilitates continual improvement and enhancement of the organization

Framework (Clause 4)

- Mandate and commitment (4.2)
- Design of framework for managing risk (4.3)
- Continual improvement of the framework (4.6)
- Implementing risk management (4.4)
- Monitoring and review of the framework (4.5)

Process (Clause 5)

- Establishing the context (5.3)
- Risk assessment (5.4)
- Risk identification (5.4.2)
- Risk analysis (5.4.3)
- Risk evaluation (5.4.4)
- Risk treatment (5.5)

Communication and consultation (6.2)
Relationship between the components of managing risk (ISO, 2009)
ISO 31000 risk management process (ISO, 2009)
Quality Assurance + Quality Control = Quality Enhancement

I want to do something (new idea, derive or next stage)

Resource

Exchange

Concept & Plan

What do you need to know? (What are you aiming for?)

Why do you need to know?

When will you know you succeeded? (How will you know?)

What are the potential risks and their consequences?

What happens when you get in trouble? What's your Plan B?

Enterprise Risk Management

Continuous improvement (Quality Control loop)

Summative evaluation process

Formative assessment & evaluation

Summative evaluation results/Performance results documentation/Quality Assurance

Strategy pursued/Processes used & how good they are to meet your needs

People's attitudes & support - colleagues, staff, stakeholders, Ethical considerations

Sector environment knowledge/Environmental scanning capacity/ Uncertainty level/ User satisfaction

Assumptions you made/External expectations of what you should be doing

It works & I can prove it

Doing it & keeping your eye on it

Oops. Doesn't work or not quite there yet or cannot properly document what we're doing
References

- Please contact me at fernando.padro@usq.edu.au for an updated list of references and links to get these.
Thank you for listening

Do you have any questions? Please feel free to ask now or email me.