Part 2: Enterprise Risk and Strategic OHS Risk Management

Risky Business at UQ

This was a combined presentation encompassing Enterprise Risk Management, the impact on how we manage OHS risk and the strategic OHS risk management mechanisms.

Suresh Chand & Naomi Kemp

March 2017
© University of Queensland
Outline

1. Definitions and Principles
2. Risk Management Strategy and Framework
3. Risk Appetite Statement (RAS) and Risk Categories
4. Controls
5. Three Lines of Defence
6. Risk Culture
What is Risk? Common responses……

1. Danger, Hazard, Threat

2. Possibility of something not going according to plan, resulting in a loss, harm or unwanted outcomes

3. A situation or activity involving exposure to danger or unwanted outcomes

4. Problems / challenges / difficulties faced while trying to do something worthwhile

5. Possibility of losing something of value while trying to gain something of (higher) value

6. Chances that actual results/ outcomes will be different from those expected /planned
Risk and Risk Management

1. Risk is the ‘effect of uncertainty on objectives’. [ISO 31000:2009]

2. OHS Risk – ‘the possibility that harm (death, injury or illness) might occur when exposed to a hazard’ (PPL).

3. In the context of risk management, uncertainty exists when there is an inadequate or incomplete information/knowledge/understanding of an event, its likelihood and/or its consequence.

4. Risk may be a single event or a set of circumstances that affect, adversely or beneficially, the achievement of objectives.

5. Risk management refers to the set of principles, framework, culture, processes and coordinated activities to direct and control an organisation with regard to the many risks that can affect its ability to achieve its objectives.

6. 0% < Uncertainty < 100%

7. Risk = effect of Uncertainty on objectives

8. Risk Management = Confidence in achieving objectives
Risk Management Obligations

In addition to the international Standard ISO 31000:2009, UQ’s risk management function is shaped by and demonstrates compliance with the following obligations relating to risk management:

1. Section 61 of the Financial Accountability Act 2009 (the Act) requires the establishment and maintenance of an **appropriate system of risk management**.

2. Section 28 of the Financial and Performance Management Standard 2009 prescribes that UQ’s risk management system must provide for mitigating the risk to the University and the State from unacceptable costs or losses associated with the operations of the University, and **managing the risks that may affect the ability of the University to continue to provide services**.

3. The Higher Education Standards Framework (Threshold Standards) 2015, made under the Tertiary Education Quality and Standards Agency Act 2011 (TEQSA Act 2011), requires that **risks to higher education operations are identified and material risks managed and mitigated effectively**.

We assess and manage our risks because it is important for our success and survival.
Our Risk Management Strategy

1. Risk management at UQ is an enabling management function overseen by the Senate and undertaken by managers and staff at all levels of the organisation and in all aspects of its operations.

2. RM helps address “uncertainty” in relation to the achievement of objectives and priorities with a view to reducing the variability of outcomes.

3. Risk management is (to be) an integral part of management thinking, discussions and decision making and help management find the right balance amongst value, cost and risk.

4. UQ’s risk management objectives are to facilitate the achievement of its strategic and operational objectives including:
   a. Value creation and protection;
   b. Effective and efficient performance and compliance; and
   c. The development, enhancement and protection of its strategic and operational capabilities.

5. The person accountable for achieving the objectives is also accountable for managing the risks (and compliance obligations) relating to those objectives.
RISK MANAGEMENT FRAMEWORK

**OBJECTIVES AND STRATEGY**
- ASSESS RISK
  - Risk management objectives, strategies, mandate & accountabilities
- VARIANCE ANALYSIS & REMEDIATION
  - Senate expectations, risk appetite & risk governance
  - Risk management objectives, strategies, mandate & accountabilities
  - External compliance obligations relating to risk management
- MONITOR AND REPORT
  - Management commitment, support, culture & relationships
  - Risk management resources, plans, processes & activities
- MITIGATE RISK
  - Risk management resources, plans, processes & activities
- RISK APPETITE
  - Senate expectations, risk appetite & risk governance

Senate expectations, risk appetite & risk governance

Management commitment, support, culture & relationships

Risk management objectives, strategies, mandate & accountabilities

External compliance obligations relating to risk management

Risk management resources, plans, processes & activities

© University of Queensland

7
Risk Appetite Statement

1. The Risk Appetite Statement (RAS) comprises a series of statements on risks that the University is willing to accept/tolerate in the pursuit of its strategic objectives.

2. The RAS is a useful means of ensuring that the senior leadership team are in alignment with regard to risk and communicates the Senate’s appetite to decision-makers across the University to assist them in making risk-based decisions.
### WILLINGNESS TO TAKE RISKS

<table>
<thead>
<tr>
<th>Zero</th>
<th>Very Low</th>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>All reasonably practical and affordable measures to eliminate the risk must be taken.</td>
<td>All reasonably practical and affordable measures to minimise the risk must be taken.</td>
<td><strong>Prefer risk mitigation to the rewards</strong> of taking risk. Safe approaches should be taken but the cost of implementing controls should be evaluated to ensure they achieve a worthwhile level of risk mitigation.</td>
<td><strong>Risk taking in order to gain reward</strong>, provided that effective measures are in place to monitor the risk and limit adverse outcomes.</td>
<td>Eager for risks to be taken in order to gain highly valued reward/s. <strong>Focus is on achieving the reward/s.</strong></td>
</tr>
</tbody>
</table>

Safety
Compliance
Reputation
Financial Sustainability
### Governance

<table>
<thead>
<tr>
<th>Legal &amp; Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td>The University ….</td>
</tr>
<tr>
<td>▪ Has a <strong>ZERO</strong> risk appetite for intentional and material breaches of statutes, regulation and professional standards including those relating to research or medical ethics. However, it is important to ensure that our approach to compliance is efficient and does not impede the achievement of our business objectives.</td>
</tr>
<tr>
<td>▪ Has a <strong>VERY LOW</strong> risk appetite for risks relating to actions that may put course accreditations and/or standards of operations in jeopardy.</td>
</tr>
<tr>
<td>▪ Has <strong>ZERO</strong> risk tolerance for criminal breaches, fraud and corruption, misuse of office or similar related activities.</td>
</tr>
<tr>
<td>▪ Wishes to encourage innovation as to how employees efficiently and effectively meet the requirements of internal policies and procedures.</td>
</tr>
</tbody>
</table>

### Safety

<table>
<thead>
<tr>
<th>The University ….</th>
</tr>
</thead>
<tbody>
<tr>
<td>▪ <strong>Aspires to ZERO harm</strong> and is open to innovation and prudent investment in strategies to protect the health and wellbeing of our staff, students and visitors with a focus on the prevention of high risk hazards.</td>
</tr>
<tr>
<td>▪ Supports a strong safety culture and expects employees to take personal responsibility for their own wellbeing.</td>
</tr>
</tbody>
</table>
Impact of the Safety Risk Appetite

1. Determine reasonably practicable

2. Context for how we will evaluate OHS risk
   a. Express level of risk – Current Risk
   b. The level of risk that is Acceptable
   c. The level at which risk is Tolerable
   d. Who makes the decisions

3. Risk Evaluation decisions
   a. Whether an activity should proceed
   b. Whether a risk needs treatment
   c. Preferred options for risk treatment
   d. Priorities for treatment

4. OHS Risk Evaluation Criteria – table in the new procedure
### Strategic vs Operational Risks

<table>
<thead>
<tr>
<th>Strategic Risk</th>
<th>Operational Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Uncertainties and untapped opportunities embedded in our <strong>strategic intent and its implementation/ execution</strong>.</td>
<td>• Operational risk is something internal or external that would impact on your <strong>ability to implement the current strategy</strong>.</td>
</tr>
<tr>
<td>• Risks that could lead to material variations in strategic goals or outcomes</td>
<td>• Operational risks are those risks associated with day-to-day activities.</td>
</tr>
<tr>
<td>• Affects organisation’s survival and growth / expansion</td>
<td>• Risks general connected with the internal resources, systems, processes, and employees of the organisation.</td>
</tr>
</tbody>
</table>
# UQ: KNOWLEDGE LEADERSHIP FOR A BETTER WORLD

## VISION

<table>
<thead>
<tr>
<th>VALUES</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pursuit of excellence</td>
</tr>
</tbody>
</table>

## PILLARS

<table>
<thead>
<tr>
<th>Learning</th>
<th>Discovery</th>
<th>Engagement</th>
<th>Enabling</th>
</tr>
</thead>
<tbody>
<tr>
<td>Students, Teaching, Learning, Successful Graduates</td>
<td>Best researchers, research leadership, research partnerships, research excellence, demonstrable benefits from research</td>
<td>Mutually beneficial relationships with business, government, the social sector and the wider community and with alumni. Strategic, respectful relationships between Indigenous and non-Indigenous people and other stakeholders; Globally connected</td>
<td>People and culture (performance based, best people, safety, diversity); Resources (financial, systems and processes, environment); Governance (structures, strategic decisions, risk and compliance)</td>
</tr>
</tbody>
</table>

## FOUNDATIONS

<table>
<thead>
<tr>
<th>Student success, coupled with employers’ conviction</th>
<th>Research – quality, integrity &amp; impact; and partnerships</th>
<th>UQ’s global connectedness</th>
<th>Culture</th>
<th>Systems, approaches &amp; structures that maximise resources available to the academic purpose</th>
<th>Alumni community</th>
</tr>
</thead>
</table>

© University of Queensland

Suresh Chand
Focus Areas for 2017

1. Attract and retain the best students, irrespective of background
2. Implement the Student Strategy
3. Diversify and grow income streams to establish a sustainable and independent financial base
4. Establish an agile, responsive and efficient university operations reflecting a One-UQ culture
5. Build engagement and strategic relationships with a broad range of local and global partners
6. Ensure UQ is recognised internationally as a leading research university that focusses on research excellence and delivers globally significant solutions

Safety?
Risks and Controls

1. **Inherent Risks** – Risks that we need to be mindful of and manage given the objective and operating environment. i.e. Risks inherent to the objectives.

2. **Inherent Risk Level** – For a given risk, its nature and size *assuming* there are no *risk-specific controls* for that risk.

3. **Managed Risk Level** (MRL) - It is the level of risk remaining after considering the total effectiveness of all the *existing controls or risk treatments* that act upon that risk.

4. **Target Risk Level** (TRL) - It is the desired (or acceptable) level of risk considering the University’s risk appetite.
Corporate OHS Risk Register

Context / Objectives

Risk Description
(indicate the nature and significance of the risk)

Existing Controls and their Effectiveness

Current Risk Level

Proposed New Controls

Target Risk Level

NOW

Inherent Risk Level

Controls tested for effectiveness

Reporting Level

Followed up to ensure they are assigned, implemented and will be effective

Consistent with RAS

© University of Queensland
Suresh Chand
## Risk Assessment, Risk Register, Risk Management Plan and Reporting Template

<table>
<thead>
<tr>
<th>Risk Title</th>
<th>Risk Category</th>
<th>Risk Owner</th>
</tr>
</thead>
</table>

### A. Risk Identification

<table>
<thead>
<tr>
<th>Context / Objective</th>
<th>Risk Description</th>
<th>Threats and Vulnerabilities</th>
<th>Consequences</th>
</tr>
</thead>
</table>

### B. Inherent Risk Level

<table>
<thead>
<tr>
<th>Managed Risk Level - MRL</th>
<th>Target Risk Level - TRL</th>
</tr>
</thead>
</table>

- L (Low), C (Common), R (Rare)
- Determined using RAS

### C. Proposed Controls / Risk Treatments to Align MRL to TRL

<table>
<thead>
<tr>
<th>USMG Member responsible for implementing proposed treatment/s</th>
<th>Date/s for full implementation</th>
</tr>
</thead>
</table>

© University of Queensland

Suresh Chand
Safety – Hierarchy of Controls

1. Eliminate the hazard. Most effective control measure and should always be considered first.

   *If the hazard cannot be eliminated completely:*

2. Substituting a less hazardous material, process or equipment.

3. Redesigning the equipment or work process.

4. Isolating the hazard through engineering – separating the worker from the hazard.

5. Administrative controls involve minimising exposure to a risk through the use of procedures or instruction. This could involve limiting the exposure time to a particular hazard such as noise or radiation.

6. Personal Protective Equipment (PPE) - often used in combination with the above measures
Control Effectiveness – Assessment Criteria

1. **CONTROL OBJECTIVES AND SCOPE** - The control is well defined with clarity of objectives and scope (both of which are aligned with the underlying reason for the control) and categorised as mandatory.

2. **DOCUMENTATION** - Control is properly documented and its operation is embedded in relevant processes/activities.

3. **UNDERSTANDING** - Managers and staff responsible for the effective operation of the control have a very good understanding of its operations and significance.

4. **RESOURCES** - Adequate resources (funds, people, system, time etc.) have been allocated and are always available to ensure the effective operation of the control.

5. **ACTUAL OPERATION** - There is verifiable and compelling evidence that the control is consistently and reliably applied and is performing as expected or designed.

6. **MONITORING** - The control is actively monitored and is also subject to annual reviews. Monitoring and review results provide reasonable assurance that the control is achieving its objectives.

Benefits from the control should be greater than the cost of the control.
**Control** - A control is any action taken by the governing body, management, staff and other parties to increase the likelihood that established objectives and goals will be achieved. Includes actions taken to manage risk/s.

Could be Directive >> **Preventive** >> **Detective** >> **Corrective**

**Core Management Functions** [sub-objectives]

1. **Planning** – Deciding in advance what to do, when to do & how to do
2. **Organizing** - Determining best allocation of people and resources
3. **Staffing** - Putting right person on right job
4. **Directing** - Leading, Guiding, Supervising & Motivating
5. **Controlling** - Standards, Measure & Evaluate Performance, Correct
6. **Budgeting**
7. **Reporting**
8. **Values, Culture**

- New Risk does not necessarily mean New Control/s
- Strengthening the outer layer makes the organisation more **resilient** (better able to deal with ‘Black Swan” or “Unknown Unkowns”)
**Top 10 Non-academic Risks (at MRL)**

1. Transformation and Adaptability
2. Legal /Regulatory Compliance
3. Project Execution
4. Financial Sustainability
5. Cost Transparency
6. Asset Utilisation
7. Foreign Market Dependency
8. Conflict of Interests
9. ‘Black Swan’ Event/s \( L_L \ L_C \)
10. Cyber Security
# Examples - UQ Risks

<table>
<thead>
<tr>
<th>Risk Title</th>
<th>Risk Description</th>
<th>IRL</th>
<th>MRL</th>
<th>TRL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transformation &amp; Adaptability</td>
<td>Risk of not being able to achieve requisite organisational transformation within the timeframe required due to lack of clarity of transformation objectives and scope, the nature and extent of changes required and the significant gaps in our culture and capabilities to see through the changes.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Execution</td>
<td>Risk of not being able to successfully execute approved projects due to multiple projects being implemented concurrently giving rise to competing priorities and diminished focus on each project, and a lack of requisite project governance and execution capabilities (people, process and systems).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Financial Sustainability</td>
<td>Risk that the University will face unsustainable financial pressures as a result of uncertainties around its revenue streams, a high, inflexible and rising cost base, and an ever increasing need for additional funds for enhancements and growth.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# Risk Matrix

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>High [4]</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>Medium [3]</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>Extreme</td>
</tr>
<tr>
<td>Low [2]</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Very Low [1]</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
</tbody>
</table>
### ‘Three Lines of Defence’

**SENIOR MANAGEMENT – CREATES THE CONTROL ENVIRONMENT**
- Demonstrates commitment to integrity and ethical values
- Exercises oversight responsibility
- Establishes structure, authority and responsibility
- Demonstrates commitment to competence and enforces accountability

---

**FIRST LINE – (‘FRONT LINE’ OPERATING MANAGEMENT)**
- **Risk Assessment** – Specifies their ‘business’ objectives and assesses risks
- **Control Activities** – Implements controls consistent with policies and procedures
- **Monitoring Activities** - Conducts ongoing and/or separate evaluations of their risks and controls and evaluates, communicates and remedies deficiencies

---

**SECOND LINE – (HEADS OF FUNCTIONS)**
The second line is essentially a management oversight function. It develops and implements enterprise-wide controls (policies and procedures) and monitors function-specific risks, controls and compliance in support of management across the whole organisation

---

**THIRD LINE – INTERNAL AUDIT**
Provides independent assurance on governance, risk, controls, compliance etc.
Risk Culture

‘Risk culture is the set of encouraged and acceptable attitudes, behaviours, discussions and decisions that embed risk into the organisation’s decision making process and risk management into its day to day operations’

ATTRIBUTES OF A RISK-AWARE CULTURE

1. Core Values practised by senior executives in daily actions – visible and consistent role modelling
2. Clear, well-communicated and understood risk strategy (risk objectives, appetite, process)
3. Continuous, constructive and respectful challenging of preconceptions, decisions and actions
4. Sharing of information, ideas and analytical insights at all levels
5. Transparent, coordinated and inclusive decision making
6. Prompt escalation and consideration of threats, risks and concerns based on their severity
7. Failures used as critical learning opportunities (Failures are unique!)
8. Appropriate respect for and focus on external stakeholders of risk (customers, market, society)
9. Incentives and rewards aligned with the success of the organisation
Caution: Risk management ....

1. Is not about avoiding risks
2. Does not eliminate all risks
3. Cannot predict or prepare us for all risks (current or future)
4. Cannot mitigate all risks without breaching the cost-benefit principle (i.e. Cost of mitigating a risk should not outweigh the benefits)
5. Cannot compensate for poor management decisions
6. Cannot be effective without leadership support (i.e. right tone at the top)
7. Cannot guarantee success (however, it can increase the chances)
Governance, Risk and Compliance

1. Objectives, Scope, Deliverables and KPIs
2. Strategy and programs for delivering outputs and outcomes
3. Legal/Regulatory Compliance Obligations
4. Risks and controls to manage those risks
5. Design and develop Policy/Procedure in conjunction with relevant stakeholders
6. Ensure requisite process and systems capabilities are in place
7. Communication, training, guidelines, assistance & advice to help develop people capabilities to implement/apply Policy/Procedure
8. Monitor and Review to assess effectiveness / efficiency of the Policy/Procedure and identify & address any material deficiencies

© University of Queensland
Suresh Chand
OHS Risk management – Strategic Level

Corporate OHS Risk Register

Monitor risk
- Prioritise Audits, Reviews & Control Checks
- Negative (Incident) & Positive (Improvement) Outcomes

Measure risk
- Compliance & Effectiveness
- Effectiveness & Continuous Improvement

Set Targets e.g. Risk Reduction

Report on risk

Set Targets e.g. Risk Reduction

Report on risk
QUESTIONS?

‘Enabling informed decisions’