Risk Management Procedures

1. LEGISLATION/ENTERPRISE AGREEMENT/POLICY SUPPORTED

   Risk Management Policy
   Tertiary Education Quality Standards Agency Act 2011 (TEQSA Act 2011)

2. PROCEDURAL DETAILS

2.1. Responsibilities

<table>
<thead>
<tr>
<th>Entity / Officer</th>
<th>Responsibilities</th>
</tr>
</thead>
</table>
| Planning and Management Committee       | (a) Advise the Vice-Chancellor on the effective management of the University's risk profile, including risk appetite, treatment and the status of individual risks; and  
(b) Enhance the cohesion, performance and culture of the University by modelling the Curtin values, and undertaking an informed and whole-of-university approach to risk aware decision-making. |
| Chief Operating Officer                 | (a) Provide executive leadership for risk management;  
(b) Provide assurance to the Vice-Chancellor on the effectiveness of the Risk Management Framework; and  
(c) Lead the Critical Incident Management Team. |
| Executive Managers                      | (a) Promote risk aware behaviours;  
(b) Monitor and review allocated strategic risks manage and provide assurance to the Vice-Chancellor;  
(c) Disclose risks approaching or exceeding risk appetite; and  
(d) Identify strategic opportunities arising from the University's risk profile. |
| Director, Risk Management               | (a) Embed the University’s agreed risk appetite and desired risk aware behaviours as part of implementing the Risk Management Framework;  
(b) Embed business continuity and critical incident management processes across the University;  
(c) Prepare reports to Planning and Management Committee, Council sub-committees and Council as required by the these procedures; and  
(d) Disclose risks approaching or exceeding risk appetite as well as opportunities. |
| Faculty, School, Portfolio and Operational area and other managers | (a) Model risk aware behaviours;  
(b) Manage operational risks including disruptive incident risk and risks arising from counterparties delivering services on behalf of the University; and  
(c) Disclose risks approaching or exceeding the risk appetite as well as opportunities. |
| Students and staff                      | (a) Apply risk thinking as part of prudent decision making every day; and  
(b) Provide continuous disclosure of areas of concern and opportunities. |

2.2. Strategic risk management

   2.2.1. Executive Managers and Council will set the University's risk appetite at least annually.

   2.2.2. Executive Managers and Council will assess and treat strategic risks including material business risks at least annually using Risk Management templates.

   2.2.3. The relevant Executive Manager (Risk Owner) will monitor and review allocated strategic risks.

   2.2.4. The Risk Management area will ensure Executive Management and Council strategic risk considerations to inform strategy, audit, governance and operational risk considerations.

   2.2.5. Executive Managers will continuously disclose risks approaching or exceeding the risk appetite or as required by the Incident Alert Matrix.
2.2.6. Executive Managers and Council will consider the effectiveness of the Risk Management Framework at least every 3 years, including consistency with TEQSA Act 2011 requirements and AS/NZS ISO 31000:2009, Risk Management - Principles and guidelines.

2.2.7. The Risk Management area will implement training programs, tools, reports, templates and processes as necessary to embed strategic risk management.

2.3. **Operational risk management**

2.3.1. Faculty, school, portfolio and operational areas will assess and treat operational risks at least annually using Risk Management templates.

2.3.2. Faculty, school, portfolio and operational managers will operate within the risk appetite set by Executive Managers and Council.

2.3.3. Managers will continuously disclose risks approaching or exceeding the risk appetite or as required by the Incident Alert Matrix.

2.3.4. The Risk Management area will identify trends and significant issues arising of operational risk considerations to inform strategic risk, audit and governance considerations.

2.3.5. The Risk Management area will implement training programs, tools, reports, templates and processes as necessary to embed operational risk management.

2.4. **Project and contract risk management**

2.4.1. Faculty, school, portfolio and operational areas will assess and treat project and contract risks using Risk Management templates.

2.4.2. Faculty, school, portfolio and operational managers will operate within the risk appetite set by Executive Managers and Council.

2.4.3. Managers will continuously disclose risks approaching or exceeding the risk appetite or as required by the Incident Alert Matrix.

2.4.4. The Risk Management area will implement training programs, tools, reports, templates and processes as necessary to assist with contract and project risk management.

2.5. **Business continuity**

2.5.1. Faculty, school, portfolio and operational areas will assess their ability to respond to and recover from disruptive incidents, conduct a risk and business impact analysis, develop response plans (business continuity plans) and train, exercise and maintain their business continuity plans at least annually using Risk Management templates.

2.5.2. Faculty, school, portfolio and operational areas will nominate a position who will coordinate their business continuity response in the event of a major disruptive incident.

2.5.3. Executive Managers and Council will consider the effectiveness of business continuity planning at least every 3 years, including consistency with ISO 22301:2012, Societal Security: Business Continuity Management Systems - Requirements.

2.5.4. The Risk Management area will implement training programs, tools, reports, templates and processes as necessary to embed business continuity planning.

2.6. **Critical incident management**

2.6.1. Executive Managers and Council will provide stewardship in times of crisis.

2.6.2. Executive Managers and Council will consider the effectiveness of critical incident management at least every 3 years, including consistency with ISO 22301:2012, Societal Security - Business Continuity Management Systems - Requirements.

2.6.3. Managers will continuously disclose incidents or risks approaching or exceeding the risk appetite or as required by the Incident Alert Matrix.

2.6.4. The Risk Management area will implement training programs, tools, reports, templates and processes as necessary to embed critical incident management.

3. **RESPONSIBILITIES**

Responsibilities are those as set out in section 2.
4. SCOPE OF PROCEDURES
These procedures apply to University Council members, students and staff.

5. DEFINITIONS
(Note: Commonly defined terms are located in the Curtin Common Definitions. Any defined terms below are specific to this document)

**Business continuity**
The capability to continue to deliver products or services at acceptable predefined levels following a disruptive event.

**Incident**
A situation that might be, or could lead to a disruption, loss, emergency or crisis.

**Operational risks**
Those operational management issues identified across Faculty, School, Portfolio or Operational areas that can affect the success of the Faculty, School, Portfolio or Operational area achieving their objectives. There are hundreds of risks at this level when combined across the University. However, to make the operational risk process manageable and meaningful, it has two key aspects:
(a) Around fifteen generic dependency-based risks relating to strategy, governance, people, safety, systems, data, business continuity, budget, etc; and
(b) Outcome-based risks that relate to the business area’s operational core functions or key services.

**Managers**
Include Faculty, Portfolio and Operational area managers, supervisors and workers with management responsibilities

**Risk appetite**
The amount and type of risk an organisation is prepared to pursue or retain to achieve its objectives. Curtin’s Risk Appetite is described in the Risk Management Policy and is detailed in Risk Reference Tables linked to this procedure.

**Risk aware**
Decisions are made in a disciplined way, taking into account considerations of risk and reward on an informed basis.

**Risk management**
Coordinated activities to direct and control an organisation with regards to risk.

**Risk Management Framework**
Set of components (which include the policy and procedures) that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.

**Risk treatment**
Agreeing and implementing options that change the likelihood and/or the consequence of a risk. Options may be to avoid the risk, reduce the risk, remove the source of the risk, modify the consequences, change the probabilities, share the risk with others, retain the risk, or you can even increase the risk in order to pursue an opportunity. Once a treatment has been implemented, it becomes a control or it modifies existing controls. There can be multiple treatments for a risk.

**Strategic risks**
Those matters that can affect the success of Curtin in achieving its strategic objectives. They include material business risks and the significant nature of these risks means that stakeholders and regulators would expect the Council to be actively monitoring them as part of its stewardship role.

6. SCHEDULES
Nil

7. RELATED DOCUMENTS/LINKS/FORMS
Incident Alert Matrix
Curtin Risk Reference Tables including Risk Appetite
Curtin’s Risk Management webpage

<table>
<thead>
<tr>
<th>Policy Compliance Officer</th>
<th>Michelle Griffiths, Director, Risk Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy Manager</td>
<td>Chief Operating Officer</td>
</tr>
<tr>
<td>Approval Authority</td>
<td>Vice-Chancellor</td>
</tr>
<tr>
<td>Review Date</td>
<td>1st April 2016</td>
</tr>
</tbody>
</table>

REVISION HISTORY

<table>
<thead>
<tr>
<th>Version</th>
<th>Approved/ Amended/ Rescinded</th>
<th>Date</th>
<th>Committee / Board / Executive Manager</th>
<th>Approval / Resolution Number</th>
<th>Key Changes and Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>New</td>
<td>Approved</td>
<td>20/02/2013</td>
<td>Vice-Chancellor</td>
<td>EM1304</td>
<td>Unconditional approval, effective 27 February 2013</td>
</tr>
<tr>
<td></td>
<td>Administratively Updated</td>
<td>06/10/2015</td>
<td>Director, Legal and Compliance Services</td>
<td>EC 76/15</td>
<td>Executive Manager Title Changes</td>
</tr>
</tbody>
</table>