Introduction

The University of Canterbury is committed to managing its risks in a proactive, on-going and positive manner. This document outlines a strategy for this process. The framework is aligned with Joint Australian/New Zealand International Standard® Risk Management – Principles and Guidelines, [AS/NZS ISO 31000:2009] (Standards New Zealand website) and key planning documents of the University. The Framework was first developed in February 2005, is approved by the Audit and Risk Committee on behalf of the University Council, and is reviewed every three years or as required.

Contents

Policy Statements ........................................................................................................2
  Risk Management ........................................................................................................2
  Legal Compliance .........................................................................................................3
Definitions ....................................................................................................................3
Guidelines ....................................................................................................................6
  1. Governance and Management ..................................................................................6
  2. Risk Management Programme ................................................................................8
     2.1 Principles .............................................................................................................8
     2.2 Approach ..........................................................................................................9
     2.3 Objectives .........................................................................................................9
     2.4 Risk Identification and Analysis .......................................................................9
     2.5 Process .............................................................................................................10
  3. Education ..............................................................................................................13
  4. Monitoring and Review .........................................................................................13
  5. Communication and Consultation ..........................................................................14
  6. Legal Compliance Programme .............................................................................14
Policy Statements

Risk Management

The University recognises that it must systematically manage and regularly update its risk profile at a strategic, operational, and project level to explicitly address uncertainty and facilitate continuous improvement. The University has committed to this by developing a risk management and compliance framework that describes the process and identifies tools for realising its objectives. Not only does UC wish to minimise its downside risks but also maximise its opportunities.

The framework’s scope is University-wide, including its trusts. The framework is aligned with Joint Australian/New Zealand International Standard® Risk Management – Principles and Guidelines, [AS/NZS ISO 31000:2009] (“the Standard”) and key University strategic, operational and project plans; together with external expectations from, for example, the Ministry of Education and the Tertiary Education Commission. It is expected that the framework will both inform and be informed by the Standard, UC’s strategic objectives and accompanying planning documents and requirements. Governance and management roles and responsibilities for risk management are documented in Section 1 of the framework.

The framework is managed by the Risk Manager with content input from those with accountability in specific areas. A Strategic Risk Register has been developed at the University strategic level that is maintained dynamically, and formally reviewed and reported on twice a year by strategic risk owners who are all members of the Senior Management Team (SMT). The Register is considered by the Senior Management Team, the Audit and Risk Committee, and the University Council. Content and recommendations are used to inform the University’s internal audit programme and subsequent iterations of the Strategic Risk Register.
Legal Compliance

As part of the risk management process, the University appreciates that one of its core risks is compliance with statutory obligations.

It is thus committed to not only identifying the legislation with which it is obliged to comply, but also monitoring the levels of compliance in the institution and implementing change and/or mitigations where necessary (see Appendix F: Relevant Legislation).

The University has developed a risk management and compliance framework, as outlined here, that details the process by which it will systematically identify, measure and improve compliance practices. One way in which this is done is by adoption of the “Three Lines of Defence” model (see Section 4: Monitoring and Review and Appendix H: Three Lines of Defence Model for further details).

Definitions


 Controls – measures employed to modify risk; the existing processes, policy, devices, practices or other actions that act to minimise negative risks or enhance positive opportunities.

 Gross Risk – the initial assessment of the impact and likelihood of a risk prior to considering any existing controls, i.e., in the absence of controls; sometimes referred to as inherent risk.

 Impact (or consequence) – the outcome of an event which impacts an objective either positively or negatively. The impact may be certain or uncertain and may be expressed qualitatively or quantitatively.

 Legal Compliance Programme – system for identifying and monitoring compliance with legislation that raises employee awareness of legal obligations and aims to embed a compliance culture in the organisation.

 Likelihood – the chance of something happening; whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically.

 Net Risk – the impact and likelihood of a risk, taking into account existing controls; sometimes referred to as residual risk. That treatment might include avoiding, modifying, sharing or retaining the risk.

 Risk – the effect of uncertainty on objectives.

A risk is not an event.

Objectives and uncertainty give rise to risk.
Particular sources of uncertainty (whether in the internal or external environment), are sometimes referred to as “risk sources”.

It is not correct to describe a hazard or some other risk source as a risk. It is also not correct to characterise a risk as “positive” or “negative” although it would be valid to describe the consequences associated with a risk as either beneficial or detrimental in terms of an organisation’s objectives.

Because risk is the effect of uncertainty on objectives, the description of risk needs to convey both elements – it needs to make clear which objectives are being referred to, the source of uncertainty and how it could lead to consequences.

The level of risk is expressed as the likelihood that particular impacts (or consequences) will be experienced. Impacts (or consequences) relate directly to objectives and arise when something does or does not happen.

Risk descriptions should make clear which objective is at risk; the source of the risk and the sequence through which the effects on the objective could be experienced.

**Risk Appetite/Tolerance** – the amount or degree of risk that an organisation is prepared to accept or pursue. To assess this, an understanding of an organisation and its context (both internal and external) must be established.

**Risk Assessment** – the overall process of identifying, analysing, and evaluating risks. It may also be referred to as a “risk analysis” or “risk evaluation” or “risk profile” and may involve a qualitative and/or quantitative assessment (see *Appendix A*).

**Risk Management** – the culture, processes, coordinated activities, and structures that are directed towards realising potential opportunities and/or managing adverse effects. The risk management process involves communicating, consulting, establishing context, identifying, analysing, evaluating, treating, monitoring and reviewing risks.

**Risk Owner** – the person or entity (e.g., Committee Chair) with the accountability and authority to manage a risk.

**Risk Register** – a documented record of each risk identified. It specifies
- a description of the risk, its causes and its impacts;
- an outline of the existing internal and external controls;
- an assessment of the consequences of the risk should it occur and the likelihood of the consequence occurring, given the controls;
- a risk rating; and
- an overall priority for the risk.

It should also identify time bound future actions or an action plan. Risk Register templates and other tools are available in SharePoint.

**Risk Treatment** – the process to modify risk (see *Section 2.4* for an explanation of what a risk treatment, or management of a risk, might involve).
Types of Risk

- **Strategic Risks** are external and internal forces that may have a significant impact on achieving key strategic objectives. The causes of these risks include such things as national and global economies and most significantly government policy. Often, they cannot be predicted or monitored through a systematic operational procedure. The lack of advance warning and frequent immediate response required to manage strategic risks means they are often best identified and monitored by senior management as part of their strategic planning and review mechanisms. Note: sometimes strategic risks are also described as business risks.

- **Operational Risks** are inherent in the ongoing activities that are performed in an organisation. These are the risks associated with such things as the day-to-day operational performance of staff, the risks inherent in the organisational structure, and the manner in which core operations are performed.

- **Project Risks** are risks associated with projects that are of a specific, sometimes short term nature and are frequently associated with new teaching and learning courses, significant new research or acquisitions, change management, integration, major IT and capital development projects. Project Sponsors are accountable for the achievement of project deliverables and outcomes. However, specific risks associated with project management are normally delegated to project managers for attention and action. Included among the benefits of efficiently managing project risks are the avoidance of unexpected time and cost overruns. In addition, when project risks are well managed, there are fewer integration problems with assimilating required changes back into general management functions.
## Guidelines

### 1. Governance and Management

Specific roles and responsibilities for risk management in the University are as follows:

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Council</td>
<td>Governance responsibility for risk management and legal compliance at the University of Canterbury.</td>
</tr>
</tbody>
</table>
| Audit & Risk Committee            | Governance oversight for risk management and legal compliance at the University of Canterbury.  
|                                   | Approval of Risk Management and Compliance Framework, on behalf of Council.          |
| Vice-Chancellor                   | Management responsibility of risk management and legal compliance.                 |
| University Registrar              | Delegated responsibility for risk management University wide: risk policy, risk monitoring, and reporting to Audit and Risk Committee (see The University Council Delegation Schedules (University of Canterbury website)).  
|                                   | Management oversight of risk management and legal compliance on behalf of the Vice-Chancellor.  
|                                   | Assessment of the levels of acceptable risk and risk treatments and recommendations to the Vice-Chancellor accordingly.  
|                                   | Monitoring of Strategic Risk Register and regularly reporting to Audit and Risk Committee on management of risk issues.  
|                                   | Risk Management “champion” for the University.                                      |
| Senior Management Team Members (SMT) | Management endorsement of Risk Management and Compliance Framework.  
|                                   | Risk owners of strategic risks within the University.  
|                                   | Strategic and operational risk assessment, management, monitoring and reporting to the University Registrar and/or the Risk Manager for all risks relative to their areas of accountability. |
| Risk Manager                      | Management of the process of identifying and monitoring risk at the University.  
|                                   | Maintenance of Strategic Risk Register.  
|                                   | Development of tools to assist the University community to implement best practice for risk and compliance matters.  
|                                   | Provision of support and training opportunities for all staff to promote a risk culture in the University.  
|                                   | Assistance with the development of Operational and Project Risk Registers.  
<p>|                                   | Publication/Dissemination of regular risk management and compliance information to keep staff informed of relevant issues and/or changes in legislation impacting statutory compliance. |</p>
<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pro-Vice-Chancellors and Service Unit Directors</td>
<td>• Identification and analysis of strategic, operational and project risks within the College/Unit; elevating risks where relevant to the Strategic Risk Register.</td>
</tr>
<tr>
<td>Project Sponsors and Project Managers</td>
<td>• Assessment, management, monitoring and reporting of relative project risks to relevant senior managers, Senior Management Team members and relevant committee/s or programme boards.</td>
</tr>
<tr>
<td>All Staff</td>
<td>• Cognisance of operational and strategic risks, including identifying and reporting increases in risks or new risks in a timely way. It is also expected that tasks will be performed in a careful and conscientious manner that reflects, but is not limited to, University policies (see UC Policy Library (University of Canterbury website)).</td>
</tr>
</tbody>
</table>
| Internal Audit Team                                                 | • Advice to senior management in the development of best practice risk management systems.  
|                                                                   | • Provision of professional independent advice on key risk and control issues, when requested.  
|                                                                   | • Regular audit reviews of the University’s risk management processes. |

While Senior Management Team members are accountable for risk management in their particular portfolios, responsibility for good risk management rests with every staff member.

See Appendix D: The Governance, Risk and Compliance Model (reproduced with permission from PricewaterhouseCoopers).
2. Risk Management Programme

2.1 Principles

The Joint Australian/New Zealand International Standard® Risk Management – Principles and Guidelines, [AS/NZS ISO 31000:2009] identifies 11 principles that it considers underpin effective risk management at all levels of an organisation (see Appendix A).

The University’s vision for risk management is to have a culture in which risk is managed in an integrated manner that will enable the University to

- be recognised as a leading university with best practice management to achieve the University’s Statement of Strategic Intent (University of Canterbury website);
- achieve financial and operational goals; and
- be seen as a university of high ethics that is managing its risks responsibly.

See Appendix G: Risk Culture Model (reproduced with permission from copyright owners, Dawson McDonald & Associates).

The successful management of risk within the University depends upon the following:

- The University’s risk management approach (embodied in this risk management and compliance framework) meeting current needs and being sufficiently robust to enable the University to achieve any significant changes required by Government (e.g., Tertiary Education Commission) and/or the tertiary sector.
- Risk management being an integral part of strategic, operational and project planning, and activities throughout all levels of the University.
- Risk management being openly accepted and supported by University leadership as providing good value, with this acceptance reinforced through avenues such as the performance requirements and assessment criteria of managers and staff (both academic and non-academic).
- Risk management being easy to incorporate into University activities and being seen as central to achieving goals and strategic targets identified in the University’s Investment Plan (TEC) and other strategic plans (University of Canterbury website).
- Risk being managed proactively in the University by knowledgeable staff using appropriate controls which are monitored regularly.

2.2 Approach

The University is committed to implementing a process by which strategic, operational and project risks (see Definitions above) are identified, communicated, monitored and regularly reported, as appropriate, to Council (or other appropriate body). To facilitate this, a risk management and compliance framework has been developed for the University that proactively and systematically identifies, monitors, and manages risks. This framework aligns with the Joint Australian/New Zealand International Standard® Risk Management – Principles and Guidelines: AS/NZS ISO 31000:2009 and is regularly reviewed and updated in consultation with the University’s internal auditor.
The risks identified will be determined and monitored by those with accountability in specific areas who will be supported by appropriate training, educative tools, and assistance from the Risk Manager. It is expected that these risks will both inform and be informed by strategic and operational plans developed at University, College, and Service Unit levels.

2.3 Objectives

The University's risk management objectives are to

- identify and manage existing and new risks in a planned and coordinated manner with the minimum of disruption and cost;
- develop a risk aware culture that encourages all staff to identify risks and associated opportunities and to respond to them with cost effective actions in a timely manner; and
- be perceived by stakeholders as a leading university through adopting best risk management and legal compliance practice.

2.4 Risk Identification and Analysis

The types of risks faced by a tertiary institution such as the University of Canterbury are many and varied, and may be categorised as strategic, operational or project type risks. These risks may impact – either beneficially or detrimentally – on the University’s human resources, environment, information management, intellectual property, image and financial assets. For a list of the sorts of risks that may be encountered, see Appendix E.

The University has five main ways in which it can effectively manage risk:

1. Accept the risk and make a conscious decision to not take any action.
2. Accept the risk but take some actions to lessen or minimise its likelihood or impact.
3. Transfer the risk to another individual or organisation, by, for example, outsourcing the activity.
4. Finance (insure against) the risk.
5. Eliminate the risk by ceasing to perform the activity causing it.

2.5 Process

The University maintains a strategic risk register that identifies and registers key strategic risks. This is maintained dynamically and formally reviewed and reported to the Audit & Risk Committee twice yearly. The Strategic Risk Register is informed by the risk registers developed at College and Service Unit levels and input from Pro-Vice-Chancellors, College Executive teams and Service Units. The latter are the responsibility of those with accountability (e.g., portfolio ownership) in these areas.

How the University decides to manage individual risks is determined following a risk assessment based on a systematic analysis of how a number of impact (or consequence)
and likelihood ratings apply to each risk. The University has identified relevant impact and likelihood ratings, as shown in Appendix B. In addition to assessing likelihood and consequence ratings, the effectiveness of existing controls over a 12 month period are also considered in terms of the ratings illustrated in Appendix B.

See Appendix C for a diagrammatic representation of an overall risk rating matrix.

The risk assessment process starts by identifying the appropriate risks. These risks may initially be rated as Gross Risks – i.e., the impact and likelihood of these risks assessed without taking into account the controls that currently exist to mitigate the risk.

After this initial assessment, the risks are re-assessed as Net Risks – i.e., taking into account the aforementioned controls and documented accordingly.

By assessing risks as both Gross and Net, we are able to make a judgement on the effectiveness of the controls in place to mitigate the risks. This is an important step in testing assumptions about the robustness of controls. It is the case, however, that strategic and operational risk registers developed at the University are typically assessed by net risk only. This is because there are generally some controls already in place for the risks identified and, in reality, it is difficult to think about risk assessment for strategic and operational risks in the absence of existing controls. This process is driven by a number of steps:

**Step 1: Linking identified risks to objectives**

The first step is to ensure that the identified risk is a risk to the realisation of the University’s Statement of Strategic Intent; the primary components of which are Challenge, Concentrate and Connect. Within each of these components are strategic objectives aligned to recruitment, retention, financial viability, teaching excellence, research quality, community engagement, campus development, Māori engagement, Pacific engagement, and continuous improvement.

**Potential Risk Categories**

- Accreditation
- Attraction and Retention of Students
- Business Continuity
- Communication
- Compliance
- Emergency Management
- Financial
- International Student Relationship Management
- IT Delivery
- Programme Delivery
Step 2: Determining the impact of the risk

The second step is to determine the impact the risk would have on the University. To achieve this, qualitative risk ratings and criteria have been agreed, as set out in Appendix B.

Four key types of possible impacts have been identified: Operational, Health and Safety, Reputational and Financial, together with five levels of impact for each type – ranging from “Minor” to “Catastrophic”.

It should be noted that each type of impact must be considered separately, and comparison is not necessarily made amongst them. For example, whilst it is suggested that a risk with an economic impact greater than $10m is catastrophic, this does not mean that the financial value of the other critical impacts (such as “serious or sustained public and media attention”) is also valued at greater than $10m or needs to be satisfied to categorise the risk as having a catastrophic impact.

Step 3: Determining the likelihood of the risk occurring

The second axis on which the risk is assessed is the likelihood of the risk occurring. The following definitions of likelihood have been agreed:

<table>
<thead>
<tr>
<th>Rating</th>
<th>%</th>
<th>Likelihood Criteria (within 12-24 months)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0-10</td>
<td>Highly unlikely to occur</td>
</tr>
<tr>
<td>2</td>
<td>10-25</td>
<td>Possibility of occurrence</td>
</tr>
<tr>
<td>3</td>
<td>25-75</td>
<td>Good possibility of occurrence</td>
</tr>
<tr>
<td>4</td>
<td>75-90</td>
<td>Likely to occur</td>
</tr>
<tr>
<td>5</td>
<td>90-100</td>
<td>Almost certain to occur</td>
</tr>
</tbody>
</table>

Step 4: Multiplying the Impact and Likelihood Ratings to produce the Risk Rating

The final step is to multiply Impact by Likelihood to produce the Overall Risk Rating.

\[
\text{Impact} \times \text{Likelihood} = \text{Overall Risk Rating}
\]
Given that we have used a five-scale rating for Impact and Likelihood, this will result in a number between 1 and 25.

<table>
<thead>
<tr>
<th>Impact</th>
<th>5</th>
<th>10</th>
<th>15</th>
<th>20</th>
<th>25</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td></td>
</tr>
</tbody>
</table>

The following definitions have been agreed to categorise the overall risk ratings:

<table>
<thead>
<tr>
<th>Rating</th>
<th>Minor</th>
<th>Moderate</th>
<th>Significant</th>
<th>Major</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>1, 2, 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4, 5, 6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8, 9, 10, 12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>15, 16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20, 25</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Key points to note when applying risk ratings**

a) Only risks that are rated “Major” or above (net risk) will be taken forward into the action planning stage at the strategic level. Risks with lower overall risk ratings, however, will still need to be monitored and reviewed by risk owners, particularly if the risk changes or the controls become vulnerable.

b) When assessing a risk (such as, “Critical ICT system failure resulting in loss of critical data”), the impact and likelihood of the risk will vary widely, depending on the exact nature of it. It is important, therefore, to detail the exact nature of the risk in the “risk context” part of the risk register. It is not practical to attempt to define all ICT system failure events that may lead to loss of data since many will not be of sufficient significance to warrant this effort.

A “major” risk rating would be achieved by any of the following:

- “Impact = 5, Likelihood = 3, Risk Rating = 15”; or
- “Impact = 3, Likelihood = 5, Risk Rating = 15”; or
- “Impact = 4, Likelihood = 4, Risk Rating = 16”.

At the action planning stage, management can then determine the risk treatment that needs to be applied to manage this risk down to a level that the organisation deems tolerable.
c) While this framework is based on a 5x5 matrix of assessment, it is appropriate from time to time to measure and document risk using the simpler 3x3 matrix of High, Medium and Low. Where this rating schema is applied, the alignment to the framework is as follows:

<table>
<thead>
<tr>
<th>3x3 Matrix</th>
<th>Equivalent 5x5 Matrix</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>[15-25]: 5x5, 5x4, 4x5, 4x4, 5x3, 3x5</td>
</tr>
<tr>
<td>Medium</td>
<td>[8-12]: 4x3, 3x4, 5x2, 2x5, 3x3, 4x2, 2x4</td>
</tr>
<tr>
<td>Low</td>
<td>[1-6]: 3x2, 2x3, 5x1, 1x5, 2x2, 3x1, 1x3, 2x1, 1x2, 1x1</td>
</tr>
</tbody>
</table>

3. Education

Creating a risk aware culture in the University is a crucial part of implementing and sustaining a robust risk management and compliance programme. In addition to providing training and support for those with portfolio responsibilities in the areas of risk and compliance, opportunities should also be provided for all staff to engage in regular training opportunities about relevant risk and compliance issues. Further, tools and/or information have been developed and assembled to raise awareness about risk management and statutory compliance obligations. These are available through SharePoint.

4. Monitoring and Review

Responsibility for monitoring and reviewing risks identified in strategic, operational and project risk registers lies with risk owners, management and governance. It is the expectation of Council that any strategic risks are brought to its attention by portfolio owners within the Senior Management Team. It is the expectation of Senior Management that any emerging/new strategic risks are brought to its attention by line management and risk owners within Colleges and Services Units.

At all times, risks should be reviewed and monitored such that the controls are evaluated and further time-bound action plans are implemented to ensure the risks are managed in a manner that ensures that the level of risk remains acceptable. In addition to nominating an appropriate timeframe, action plan items should be assigned to “action owners” with operational responsibility for implementation of the actions documented in the risk register. This is not a static process that occurs at a fixed date, but rather is dynamic and responsive to changes in the University’s objectives and its environment.

The University uses the Three Lines of Defence Model for managing its risks whereby the first line of defence is internal controls at the line management level; the second line of defence is at senior management level; and the third line of defence is independent and at governance level (see Appendix H: Three Lines of Defence Model and the Institute of Internal Auditors’ Position Paper, “The Three Lines of Defense in Effective Risk Management and Control”, January 2013).
5. Communication and Consultation

Risk Management cannot exist as a separate activity. To be effective, it must be integrated into an organisation's “business as usual”. As described in the Standard, all aspects of managing risk involve people. Both internal and external stakeholders, therefore, need to be informed about, and consulted on, any risks impacting University objectives.

The Risk Manager regularly engages with risk owners across the organisation and consults with the University Registrar and Vice-Chancellor in developing reports, which are formally conveyed biannually in full or in summary, to the Senior Management Team, the Audit and Risk Committee and University Council. From time to time, strategic risks are raised outside the formal reporting periods and these are brought to the attention of management and governance, as matters of urgency, as appropriate.

In addition, the Vice-Chancellor provides the Council with situational reports (SIT Reps) on short and medium term risks each month. These reports are based on the Vice-Chancellor’s assessment of the trend within those risks. They align with the Strategic Risk Register and also provide an opportunity to look ahead and/or raise awareness about new or emerging risks.

A mature risk culture will be embedded over time through on-going education, the provision of risk tools and the regular publication of risk management updates, particularly as they pertain to changes in legislation.

6. Legal Compliance Programme

In the process of determining strategic risks impacting both positively and negatively on the business processes of the University, a readily identifiable strategic risk is related to the level and acceptability of compliance with legislative requirements. A legal compliance programme must therefore be an integral part of the Risk Management and Compliance Framework. It need not, however, be managed separately.

The University is obliged to comply with a number of legislative requirements as laid down in various Acts (see Appendix F for a list of the relevant legislation).
Related Documents and Information

Legislation

See Appendix F for relevant legislation.

UC Policy Library

- UC Policy Library (University of Canterbury website)

UC Website and Intranet

- Statement of Strategic Intent (University of Canterbury website)
- The University Council Delegation Schedules (University of Canterbury website)
- University Plans (University of Canterbury website)

External

- Three Lines of Defence Model (Office of the Controller and Auditor-General of New Zealand website)

Appendices

- Appendix B: UC Risk Impact Criteria and Likelihood Ratings
- Appendix C: Overall Risk Rating Matrix
- Appendix D: The Governance, Risk and Compliance Model – reproduced with permission from PricewaterhouseCoopers
- Appendix E: Types of Risks
- Appendix F: Relevant Legislation
- Appendix G: Risk Culture Model – reproduced with permission from copyright owners, Dawson McDonald & Associates
- Appendix H: Three Lines of Defence Model (Office of the Controller and Auditor-General of New Zealand website)
<table>
<thead>
<tr>
<th>Version</th>
<th>Action</th>
<th>Approval Authority</th>
<th>Action Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.00</td>
<td>Framework developed.</td>
<td>Chair, Council</td>
<td>Feb 2005</td>
</tr>
<tr>
<td>2.00</td>
<td>Full Review.</td>
<td>Deputy Vice-Chancellor</td>
<td>Feb 2008</td>
</tr>
<tr>
<td>3.00</td>
<td>Review to align with new standard: AS/NZS/ISO31000.</td>
<td>Chair, SMT</td>
<td>Jul 2010</td>
</tr>
<tr>
<td>3.01</td>
<td>Minor amendments to lines of responsibility (Section 1).</td>
<td>Chair, Audit &amp; Risk Committee</td>
<td>Aug 2010</td>
</tr>
<tr>
<td>4.00</td>
<td>Full Review.</td>
<td>Audit &amp; Risk Committee</td>
<td>Aug 2013</td>
</tr>
<tr>
<td>4.01</td>
<td>Minor amendment to Appendix B.</td>
<td>Audit &amp; Risk Committee</td>
<td>Oct 2013</td>
</tr>
<tr>
<td>4.02</td>
<td>Change to C/O title.</td>
<td>Policy Unit</td>
<td>May 2014</td>
</tr>
<tr>
<td>4.03</td>
<td>C/O title updated throughout document.</td>
<td>Policy Unit</td>
<td>Mar 2015</td>
</tr>
<tr>
<td>4.04</td>
<td>Minor formatting change.</td>
<td>Policy Unit</td>
<td>Mar 2015</td>
</tr>
<tr>
<td>5.00</td>
<td>Full Review.</td>
<td>Audit &amp; Risk Committee</td>
<td>Sep 2016</td>
</tr>
<tr>
<td>5.01</td>
<td>Changed title of Contact Officer from Senior Risk &amp; Insurance Advisor to Risk Manager.</td>
<td>Policy Unit</td>
<td>Jan 2017</td>
</tr>
</tbody>
</table>
Appendix A:
(Reproduced from Figure 1 of AS/NZS ISO 31000:2009 with the permission of Standards New Zealand under License 000784)
## Appendix B: Risk Impact and Likelihood Criteria

<table>
<thead>
<tr>
<th>Rating</th>
<th>Impact Criteria</th>
<th>Financial</th>
<th>Risk Management &amp; Compliance Framework v. 5.01</th>
<th>Page 18 of 27</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Minor</td>
<td>- Minor reduction of students [8]. Undesired loss of staff member [1]. Minor impact on organisational strategic goals and operational activities.</td>
<td>Less than $100k in any 12 month period.</td>
<td>© This document is the property of the University of Canterbury. Once printed this document is considered an uncontrolled version. For the official, current version refer to the UC Policy Library.</td>
<td></td>
</tr>
<tr>
<td>2. Moderate</td>
<td>- Moderate reduction of students [80]. Undesired loss of staff members [10]. Moderate impact on organisational strategic goals and operational activities.</td>
<td>$100k to $1m in any 12 month period.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Significant</td>
<td>- Undesirable reduction of staff and students in a course. Undesired loss of an academic course. Significant impact on organisational strategic goals and operational activities.</td>
<td>$1m to $5m in any 12 month period.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Major</td>
<td>- Undesirable reduction of staff and students in a programme. Undesired loss of an academic programme. Organisational strategic goals and operational activities are impacted such that there is an undesired loss of staff and curtailment of activities.</td>
<td>$5m to $10m in any 12 month period.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Catastrophic</td>
<td>- Undesirable reduction of staff and students in a College, threatening the viability of multiple programmes. Undesired loss of a College. Organisational strategic goals and operational activities are impacted such that there is an undesired loss of staff and closure of multiple units.</td>
<td>Greater than $10m in any 12 month period.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Likelihood Criteria

<table>
<thead>
<tr>
<th>Rating</th>
<th>%</th>
<th>Likelihood Criteria (within 12-24 months)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0 - 10</td>
<td>Highly unlikely to occur</td>
</tr>
<tr>
<td>2</td>
<td>10 - 25</td>
<td>Possibility of occurrence</td>
</tr>
<tr>
<td>3</td>
<td>25 - 75</td>
<td>Good possibility of occurrence</td>
</tr>
<tr>
<td>4</td>
<td>75 - 90</td>
<td>Likely to occur</td>
</tr>
<tr>
<td>5</td>
<td>90 - 100</td>
<td>Almost certain to occur</td>
</tr>
</tbody>
</table>

### Risk Rating = Impact * Likelihood

<table>
<thead>
<tr>
<th>Impact</th>
<th>Likelihood 1</th>
<th>Likelihood 2</th>
<th>Likelihood 3</th>
<th>Likelihood 4</th>
<th>Likelihood 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>15</td>
<td>20</td>
<td>25</td>
<td>16</td>
<td>20</td>
</tr>
<tr>
<td>4</td>
<td>12</td>
<td>16</td>
<td>20</td>
<td>15</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>9</td>
<td>12</td>
<td>15</td>
<td>10</td>
<td>15</td>
</tr>
<tr>
<td>2</td>
<td>6</td>
<td>8</td>
<td>10</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>1</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>2</td>
<td>5</td>
</tr>
</tbody>
</table>

September 2013

Note: * Near misses are not generally reported to Ministry of Business, Innovation & Employment (MBIE) / + This reporting criteria is over and above the initial emergency callout
## Appendix C: Overall Risk Rating Matrix

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Likely (4)</td>
<td>Moderate (4)</td>
<td>Significant (8)</td>
<td>Significant (12)</td>
<td>Major (16)</td>
<td>Catastrophic (20)</td>
<td></td>
</tr>
<tr>
<td>Good Possibility (3)</td>
<td>Minor (3)</td>
<td>Moderate (6)</td>
<td>Significant (9)</td>
<td>Significant (12)</td>
<td>Major (15)</td>
<td></td>
</tr>
<tr>
<td>Possible (2)</td>
<td>Minor (2)</td>
<td>Moderate (4)</td>
<td>Moderate (6)</td>
<td>Significant (8)</td>
<td>Significant (10)</td>
<td></td>
</tr>
<tr>
<td>Highly Unlikely (1)</td>
<td>Minor (1)</td>
<td>Minor (2)</td>
<td>Minor (3)</td>
<td>Moderate (4)</td>
<td>Moderate (5)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minor (1)</td>
<td>Moderate (2)</td>
<td>Significant (3)</td>
<td>Major (4)</td>
<td>Catastrophic (5)</td>
<td></td>
</tr>
</tbody>
</table>

### Severity

- **(20-25)** Catastrophic and Major
  - Risk Treatment Strategies to be implemented by Directors/College Managers and action taken reported to the Risk Manager for consolidation and reporting to SMT.
- **(15-16)**
- **(8-12)** Significant
  - Risk Treatment Strategies to be implemented by Directors/Colleges Managers.
- **(4-6)** Moderate and Minor
  - Acceptable – to be managed under normal control procedures.
- **(1-3)**

© This document is the property of the University of Canterbury.
Once printed this document is considered an uncontrolled version. For the official, current version refer to the UC Policy Library.
Appendix D: Governance, Risk and Compliance Model

This model informs discussions around risk and the purpose of risk management. In moving towards an effective risk management process, the model illustrates three key activities and the surrounding cultural, technology and emerging requirements expected of stakeholders.

Reproduced with permission from PricewaterhouseCoopers
Appendix E: Types of Risk

Sources of Risk

When identifying risks, all sources of potential risk should be considered. Some sources of risk are generic to all organisations. These include:

People Risks, including:
- Human Resource Management practices
- Recruitment
- Induction
- Training & Development
- OH&S (occupational health and safety)
- OH&S Management Systems
- Hazard Management
- Industrial Action
- Manual Handling
- Health
- Rehabilitation
- EEO (equal employment opportunities)
- Fraud, Corruption & Crime

Environmental Risks, including:
- Natural Hazards
- Technological Hazards
- Security
- Hazardous and Toxic Materials (e.g., chemicals, asbestos, gas, etc.)
- Public health (e.g., Legionella, food safety, etc.)
- Emergency / Disaster Management
- Environment
- Waste and Refuse
- Radiation

Organisational Management Risks, including:
- Finance
- Insurance
- Public Liability
Other sources of risk are specific to the institution or organisation. Within a tertiary institution these might include:

**Tertiary Institution Specific Risks:**
- Educational / Teaching Operations (distance, on-campus, online, etc.)
- Research Activities
- Copyright and Intellectual Property
- Technical Operations
- Faculties and Schools
- Administrative Divisions
- Overseas Partnerships and Activities
- Government Education Policy
- Academic and Research Reputation
- Community Credibility
- Grants
- Bequests
- Overseas Students
- Student Liability
- Home Visits (Psychology, Social Work, Nursing & Mental Health students), Industry / field visits (Engineering, etc.) and work placements.

[Ian Manock *Managing Risk in Tertiary Education Institutions* (Charles Sturt University, Australia, June 2001)]
Appendix F: Relevant Legislation

- Animal Welfare Act 1999 (New Zealand Legislation website)
- Anzac Day Act 1966 (New Zealand Legislation website)
- Arbitration Act 1996 (New Zealand Legislation website)
- Biosecurity Act 1993 (New Zealand Legislation website)
- Building Act 2004 (New Zealand Legislation website)
- Canterbury Earthquake (Historic Places Act) Order 2011 (New Zealand Legislation website)
- Charities Act 2005 (New Zealand Legislation website)
- Civil Defence Emergency Management Act 2002 (New Zealand Legislation website)
- Companies Act 1993 (New Zealand Legislation website)
- Commerce Act 1986 (New Zealand Legislation website)
- Consumer Guarantees Act 1993 (New Zealand Legislation website)
- Copyright Act 1994 (New Zealand Legislation website)
- Crown Entities Act 2004 (New Zealand Legislation website)
- Designs Act 1953 (New Zealand Legislation website)
- Education Act 1989 (New Zealand Legislation website)
- Electronic Transactions Act 2002 (New Zealand Legislation website)
- Employment Relations Act 2000 (New Zealand Legislation website)
- Fair Trading Act 1986 (New Zealand Legislation website)
- Financial Markets Conduct Act 2013 (New Zealand Legislation website)
- Financial Reporting Act 2013 (New Zealand Legislation website)
- Goods and Services Tax Act 1985 (New Zealand Legislation website)
- Government Superannuation Fund Act 1956 (New Zealand Legislation website)
- Hazardous Substances and New Organisms (HSNO) Act 1996 (New Zealand Legislation website)
- Health Act 1956 (New Zealand Legislation website)
- Health and Safety at Work Act 2015 (New Zealand Legislation website)
- Heritage New Zealand Pouhere Taonga Act 2014 (New Zealand Legislation website)
- Holidays Act 2003 (New Zealand Legislation website)
- Human Rights Act 1993 (New Zealand Legislation website)
- Immigration Act 2009 (New Zealand Legislation website)
- Income Tax Act 2007 (New Zealand Legislation website)
• KiwiSaver Act 2006 (New Zealand Legislation website)
• Land Transport Management Act 2003 (New Zealand Legislation website)
• Local Authorities (Members’ Interests) Act 1968 (New Zealand Legislation website)
• Local Government Act 2002 (New Zealand Legislation website)
• Local Government Official Information and Meetings Act 1987 (New Zealand Legislation website)
• Occupiers’ Liability Act 1962 (New Zealand Legislation website)
• Official Information Act 1982 (New Zealand Legislation website)
• Ombudsmen Act 1975 (New Zealand Legislation website)
• Parental Leave and Employment Protection Act 1987 (New Zealand Legislation website)
• Patents Act 2013 (New Zealand Legislation website)
• Plumbers, Gasfitters and Drainlayers Act 2006 (New Zealand Legislation website)
• Privacy Act 1993 (New Zealand Legislation website)
• Protected Disclosures Act 2000 (New Zealand Legislation website)
• Public Bodies Contracts Act 1959 (New Zealand Legislation website)
• Public Finance Act 1989 (New Zealand Legislation website)
• Public Records Act 2005 (New Zealand Legislation website)
• Residential Tenancies Act 1986 (New Zealand Legislation website)
• Resource Management Act 1991 (New Zealand Legislation website)
• Smoke-free Environments Act 1990 (New Zealand Legislation website)
• Social Security Act 1964 (New Zealand Legislation website)
• State Owned Enterprises Act 1986 (New Zealand Legislation website)
• State Sector Act 1988 (New Zealand Legislation website)
• Student Loan Scheme Act 2011 (New Zealand Legislation website)
• Trade Marks Act 2002 (New Zealand Legislation website)
• University of Canterbury Act 1961 (New Zealand Legislation website)
• Volunteers Employment Protection Act 1973 (New Zealand Legislation website)
• Wages Protection Act 1983 (New Zealand Legislation website)
• Waitangi Day Act 1976 (New Zealand Legislation website)

Updated: 20 July 2016
Appendix G: Risk Culture Model

© 2006 - 2012 Dawson McDonald & Associates

Reproduced with permission from copyright owners, Dawson McDonald & Associates
Appendix H: Three Lines of Defence Model

As noted by the Office of the Auditor-General of New Zealand, “the ‘three lines of defence’ model is useful as a clear and effective way to strengthen communications on risk management, assurance, and control by clarifying essential roles and duties for various parts of governance, management, and day-to-day operations.”

Reproduced from the Office of the Controller and Auditor-General of New Zealand website.