Introduction

The University is committed to managing its risks in a proactive, on-going and positive manner. This document outlines a strategy for this process. This Framework is aligned with international best practice 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......................................................................................................................................2
Definitions..................................................................................................................................................3
1. Governance and Management ...........................................................................................................5
2. Risk Management Programme ...........................................................................................................7
  2.1 Principles .........................................................................................................................................7
  2.2 Approach .........................................................................................................................................8
  2.3 Objectives .......................................................................................................................................8
  2.4 Risk Appetite ....................................................................................................................................8
  2.5 Risk Identification and Analysis .......................................................................................................9
  2.6 Process .......................................................................................................................................... 9
3. Education ............................................................................................................................................ 13
4. Monitoring and Review .......................................................................................................................13
  5 Communication and Consultation ......................................................................................................14
6. Legal Compliance Programme ..........................................................................................................14

Appendices................................................................................................................................................15
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 the University 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 International Standard Risk Management – Guidelines, [ISO 31000:2018 (International Organization for Standardization website)](International Organization for Standardization website), AS/NZ ISO 31000:2009 Risk Management Principles and Guidelines (Standards NZ website) (both referred to as “the standards”) 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 standards, the University’s strategic objectives and accompanying planning documents and requirements. Governance and management roles and responsibilities for risk management are documented in the Guidelines section.

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 regularly by strategic risk owners who are all members of the Senior Management Team (SMT). The Register is considered by the Senior Management Team, the Risk Advisory Committee, 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.

1 The ISO released revised standards in 2018 but this has not been formally adopted by Standards NZ. Therefore both standards are referred to.
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.

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 A: 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 See Appendix E).

**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 C).

**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 2.5) 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>Council</th>
<th>• Governance responsibility for risk management and legal compliance at the University of Canterbury.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audit &amp; Risk Committee</td>
<td>• Governance oversight for risk management and legal compliance at the University of Canterbury.</td>
</tr>
<tr>
<td></td>
<td>• Approval of Risk Management and Compliance Framework, on behalf of Council.</td>
</tr>
<tr>
<td>Risk Advisory Committee</td>
<td>• Provision of risk advice and support to University management and governance committees about strategic, operational, and project risk.</td>
</tr>
<tr>
<td></td>
<td>• Management responsibility for implementation of the Risk Management and Compliance Framework.</td>
</tr>
<tr>
<td>Vice-Chancellor</td>
<td>• Management responsibility of risk management and legal compliance.</td>
</tr>
<tr>
<td></td>
<td>• Chair of Risk Advisory Committee.</td>
</tr>
<tr>
<td>University Registrar</td>
<td>• Delegated responsibility for risk management University wide: risk policy, risk monitoring, and reporting to Audit and Risk Committee (see <a href="#">The University UC Council Delegations</a>).</td>
</tr>
</tbody>
</table>
## Risk Management Team Members (SMT)

- 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.
- Publication/Dissemination of regular risk management and compliance information to keep staff informed of relevant issues and/or changes in legislation impacting statutory compliance.

## Pro-Vice-Chancellors and Service Unit Directors

- Identification and analysis of strategic, operational and project risks within the College/Unit; elevating risks where relevant to the Strategic Risk Register.

## Project Sponsors and Project Managers

- Assessment, management, monitoring and reporting of relative project risks to relevant senior managers, Senior Management Team members and relevant committee/s or programme boards.

## All Staff

- 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)).

## 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 B: 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 C).

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 strategic objectives,
- achieve financial and operational goals, and
- be seen as a university of high ethics that is managing its risks responsibly.

See Appendix D: 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 Governance 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 International Standard Risk Management – Guidelines: [ISO 31000:2018] (International Organization for Standardization website) and is regularly reviewed and updated.

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

- Promote consistent ‘risk-informed’ decision making aligned to the University’s strategic aims;
- 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;
- Be perceived by stakeholders as a leading university through adopting best risk management and legal compliance practice.

2.4 Risk Appetite

A risk appetite statement influences and guides decision making, clarifies strategic intent and helps to ensure choices align with the strategic plan and direction of the University.

In order to manage and achieve the University Plans (University Governance website) it is necessary for both Governance and Management to know what degree of risk they are prepared to countenance in order to achieve the Plan. As such, defining a low risk appetite in certain areas is just as important as having a high risk appetite in other areas.

The University’s risk appetite statement is as follows:

The University will have a high appetite for risk in respect of strategic growth, teaching innovation and research initiatives. In order to achieve this, it will endorse
and promote award-winning research and innovative teaching programmes in fit-for-purpose facilities that attract world class students and staff.

The University will have a low appetite for risk where the probability for regret is high because there is a likelihood of significant reputational damage; financial damage; harm to students, staff, visitors or other stakeholders; non-compliant or unethical conduct or consequences

It is accepted and expected that this risk appetite statement can only provide reasonable and not absolute assurance about strategic direction or against material breaches/loss. Further, it is expected that the University will be sufficiently flexible and nimble from time to time to step outside the parameters set by this risk appetite statement in pursuit of a desired outcome but always ensuring that a high standard of delivery quality is maintained.

It is also the case that risk appetite may be more or less prescriptive at the strategic and operational levels of the University.

The framework that supports the Risk Appetite Statement can be found in Appendix E. It demonstrates the types of threats and opportunities that inform tolerances within the risk appetite.

2.5 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 F.

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.

2.6 Process

The University maintains a strategic risk register that identifies and registers key strategic risks. This is maintained dynamically and formally reviewed and reported, in part or in full, to the Audit & Risk Committee quarterly. 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 G. 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 G.

See Appendix H 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
- Health, Safety and Wellbeing
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 H.

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 $20m 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 $20m 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>
</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>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:
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 the Risk Advisory Committee and/or 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 A: 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, the Vice-Chancellor and the Risk Advisory Committee in developing reports, which are formally conveyed quarterly in full or in summary, to the Senior Management Team, the Risk Advisory Committee, 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.

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 I) for a list of the relevant legislation).
Related Documents and Information

Legislation

See Appendix I for relevant legislation.

UC Policy Library

- UC Policy Library (University of Canterbury website)

UC Website and Intranet

- Statement of Strategic Intent (University of Canterbury Governance website)
- The University UC Council Delegations Schedule (University of Canterbury Governance website)
- University Plans (University of Canterbury Governance website)

External

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

Appendices

- Appendix A: Three Lines of Defence Model (Office of the Controller and Auditor-General of New Zealand website)
- Appendix B: The Governance, Risk and Compliance Model – reproduced with permission from PricewaterhouseCoopers
- Appendix C: Risk Culture Model – reproduced with permission from copyright owners, Dawson McDonald & Associates
- Appendix E: Risk Appetite Summary
- Appendix F: Types of Risks
• **Appendix G**: UC Risk Impact Criteria and Likelihood Ratings
• **Appendix H**: Overall Risk Rating Matrix
• **Appendix I**: Relevant Legislation

## Document History and Version Control Table

<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>
<tr>
<td>5.02</td>
<td>CO referenced an updated ISO standard via footnote, addition of relevant legislation</td>
<td>Policy Unit</td>
<td>April 2018</td>
</tr>
<tr>
<td>5.03</td>
<td>Unscheduled review, inclusion of risk appetite statement, re-ordering of appendices, minor content changes</td>
<td>Policy Unit</td>
<td>Nov 2018</td>
</tr>
<tr>
<td>5.04</td>
<td>Unscheduled review by Contact Officer, minor changes to procedural information to reflect the approved Risk Advisory Committee functions</td>
<td>Policy Unit</td>
<td>Sep 2019</td>
</tr>
</tbody>
</table>
Appendix A: 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.”

![Three Lines of Defence Diagram](image)

Reproduced from the [Office of the Controller and Auditor-General of New Zealand website](http://www.audit.nz).
Appendix B: 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.

![Governance, Risk and Compliance Model Diagram]

Reproduced with permission from PricewaterhouseCoopers
Appendix C:

(Reproduced from Figure 1 of AS/NZS ISO 31000:2009 with the permission of Standards New Zealand under License 000784)
Appendix D: Risk Culture Model

RISK CULTURE MODEL

RISK CULTURE PYRAMID

Enterprise-Wide Risk Focus - Managing risk is seen as a core element of success not merely a compliance process

Engagement – Managing risk is seen as a personal responsibility, integral to decision making and part of performance evaluation

Risk as a Priority – Managing Risks is widely perceived as a priority for successful operation

Workplace Behaviours – Aberrant behaviours (e.g. bullying, personal agendas, fraud and corruption) that adversely impact on Risk Culture are not acceptable

Communication – There are clear two way communication lines around Risk Management. Feedback is welcomed and bad news is not suppressed

Support – The organisation actively provides resources, training and support needed for positive risk culture to flourish

Leadership – Executives lead Risk Management by example, hold people accountable and encourage “champions” of Risk Management

Risk Management Strategy drives...

Policies

Procedures

Systems

Organisational Culture drives...

Values

Practices

Behaviours

Correct Treatment of Risk

Actual Treatment of Risk

Danger! If Culture is not fully aligned with Risk Strategy, Culture wins - you lose.

© 2008 - 2012 Dawson McDonald & Associates

Reproduced with permission from copyright owners, Dawson McDonald & Associates
Appendix E: Risk Appetite Summary

The following demonstrates the types of threats and opportunities that may inform the tolerances within the risk appetite, noting that these are, in practice, on a continuum that runs from a conservative (low appetite) to an entrepreneurial/innovative (high appetite) view of risk.

<table>
<thead>
<tr>
<th>Risk Appetite Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
</tr>
<tr>
<td>Low Appetite</td>
</tr>
<tr>
<td>Accept little or zero risk, taking a cautious approach towards taking risk</td>
</tr>
<tr>
<td>Strategic Growth</td>
</tr>
<tr>
<td>Financial</td>
</tr>
<tr>
<td>Compliance</td>
</tr>
<tr>
<td>Health &amp; Safety</td>
</tr>
<tr>
<td>Reputation</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Teaching Accreditation</strong></td>
</tr>
<tr>
<td>Programme and Course Development</td>
</tr>
<tr>
<td>Research Quality</td>
</tr>
<tr>
<td>Research Initiatives</td>
</tr>
</tbody>
</table>

Risk Management & Compliance Framework v. 5.04  Page 21 of 31

© This document is the property of the University of Canterbury. © This document is the property of the University of Canterbury. It has been approved at an institutional level by the relevant authority in accordance with the Metapolicy. Once printed this document is considered an uncontrolled version. For the official, current version refer to the UC Policy Library.
In order to manage and achieve the University of Canterbury’s Strategic Plan it is necessary for both Governance and Management to know what degree of risk they are prepared to countenance in order to achieve the Plan. As such, defining a low risk appetite in certain areas is just as important as having a high risk appetite in other areas.

**Strategic Growth Risk**

The strategic growth of the University is predicated on its *Statement of Strategic Intent* as articulated in the Investment Plan. In order to achieve this, the University considers that it has a **high** appetite for risk in this area. One example is the programmes of work underway to realise a number of transformational objectives that support a world class learning environment that enables students and staff to be people “prepared to make a difference – tangata tū, tangata ora”.

**Financial Risk**

The impacts of the seismic activity of 2010 and beyond continue to be felt by UC. While government support, earthquake insurance, and a return to near pre-quake student numbers have significantly improved our financial position from that of five years ago, we continue to track with prudent caution. On balance, therefore, the University considers its risk appetite in this area to be **moderate** in nature, leaning more towards low than high. This does not mean, however, that we reject growth opportunities that help realise our strategic objectives but rather that we carefully scrutinize the threats and opportunities that present with such opportunities to ensure that the University remains financially sustainable.

**Compliance Risk**

The University recognises its compliance obligations through its regulations and policies. It has low appetite for any breaches that have a material consequence in statute, regulation, professional standards, accrediting bodies, research ethics, bribery or fraud. The University considers that it has a **low** appetite for risk in this area.

**Health & Safety Risk**

Under the Health & Safety at Work Act 2015, the University acknowledges its obligations as a Person in Control of a Business or Undertaking (PCBU). Further, it anticipates that staff, students and visitors should expect that this is a safe place to work and study. The University thus considers that it has a **low** appetite for risk in this area. It aims for zero harm and has low tolerance for any University activities or actions that result in death or serious harm.

**Reputation Risk**

While the University has little appetite for sustained media attention that damages its reputation, it does support initiatives that promote its mission to contribute as a world class teaching and research university to wider societal objectives of economic development, social and community development, and environmental enhancement. The University, therefore, considers its risk appetite in this area to be **moderate** in nature.
Teaching Risk
As a university, we are ambitious and innovative in the development of new programmes and courses, and the redevelopment of current ones, but we will not compromise quality or our accreditation status in the process.

Teaching Quality
The University’s reputation as a tertiary education provider that delivers high quality programmes and attracts the very best academics and students is predicated on its strong reputation in the market. Quality assurance processes are sound, delivery quality is both expected and celebrated, and choice of pedagogy is measured. The University thus considers that it has a low to moderate appetite for risk in this area.

Teaching Accreditation Processes
Professional degree programmes at UC are bound by accreditation processes that largely determine content and delivery. UC will not compromise its accreditation by attempting to step outside the guidelines/requirements recommended by professional bodies like EngNZ and the New Zealand Speech-Language Therapists’ Association. The University, therefore, considers that it has a low appetite for risk in this area.

Programme and Course Development
As a point of difference, the University has developed a Graduate Profile that describes the attributes that UC graduates will be able to develop during their course of study. These attributes are bicultural competence and confidence; community engagement; employability, innovation and enterprise; and global awareness. In working towards these attributes, UC is exploring innovative teaching programmes, using flexible delivery options, and working in a built environment that is increasingly tailored for disruptive technologies. The University believes its tolerance for risk is higher here and thus considers that it has a high appetite for risk in this area.

Research Risk

Research Quality
The quality and quantity of research outputs underpins the successful attraction of funding, researchers and postgraduate students. While that research needs to be cutting edge to be seen as relevant, it must be driven by very high quality assurances processes. These are manifested through PBRF ratings, university rankings, publications, and compliance obligations of the likes of the Ethics Committees and regulatory bodies like the Ministry of Primary Industries (MPI). The University considers its risk appetite in this area to be largely moderate in nature.

Research Initiatives
UC is ranked 231 in the QS World University Rankings and has 15 subjects in the world’s top 200 (QS World University Rankings 2018). It continues to equal or set new targets with research revenue, research funding, postgraduate student growth, and innovative collaborative research opportunities. The University considers that it has a high appetite for risk in this area.

*The Risk Appetite Summary has been developed from the research of a number of international risk appetite models but with particular reference to Central Queensland University, Australia; the University of the Sunshine Coast, Australia; the University of Edinburgh, Scotland; and the University of Waterloo, Canada*
Appendix F: 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
- Legal Relationships
- Projects
- International Economics
- Market Competition
- Commercial / Business / Contractual / Consultancy Activities and Interruptions
- Property and Physical Assets
- Fleet
- Information Technology / Computer Systems
- Business Continuity Resumption

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 G: Risk Impact and Likelihood Criteria

<table>
<thead>
<tr>
<th>Rating</th>
<th>Operational Impact Criteria</th>
<th>Health and Safety Impact Criteria</th>
<th>Reputational Impact Criteria</th>
<th>Financial Impact Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Student number or teaching and/or research impact</td>
<td>Degree of Harm</td>
<td>Level of Interest</td>
<td>$ Value</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>Incident requiring moderate medical attention. Event report submitted to Health and Safety.</td>
<td>Moderate public or local interest. Event that involves College Manager/Direct Report management time.</td>
<td>$100k to $5m in any 12 month period.</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>Incident requiring significant medical attention. Event report &amp; investigation submitted to Health and Safety. Assault of a student or staff member.</td>
<td>Significant public or local interest. Event that involves PVC/AVC management time. Allegation of fraud/misconduct.</td>
<td>$5m to $10m in any 12 month period.</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>Serious harm event or near miss. Event report submitted to Health and Safety. Event investigation submitted to Health &amp; Safety. Serious harm event reported to Ministry of Business, Innovation &amp; Employment or other relevant authority by Health &amp; Safety Manager*. Student/Staff fatalities (off campus and non UC related activity).</td>
<td>Major public or media attention. Event that involves VC/ Audit &amp; Risk Committee management time. Fraud by staff or contractor.</td>
<td>$10m to in any 12 month period.</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>Student/Staff fatalities (on campus or off campus UC related activity). Report to Ministry of Business, Innovation and Employment or other relevant authority by the Health &amp; Safety Manager*. Event report submitted to Health and Safety. Event investigation submitted to Health &amp; Safety.</td>
<td>Serious or sustained public and media attention. Event that involves significant, unplanned and urgent Council management time. Criminal investigation of one or more members of Council/SMT.</td>
<td>Greater than $20m in any 12 month period.</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>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>4</td>
<td>6</td>
<td>8</td>
<td>10</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>6</td>
<td>9</td>
<td>12</td>
<td>15</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>8</td>
<td>12</td>
<td>16</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>10</td>
<td>15</td>
<td>20</td>
<td>25</td>
</tr>
</tbody>
</table>

August 2019

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 H: Overall Risk Rating Matrix

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Almost Certain (5)</th>
<th>Likely (4)</th>
<th>Good Possibility (3)</th>
<th>Possible (2)</th>
<th>Highly Unlikely (1)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Moderate (5)</td>
<td>Moderate (4)</td>
<td>Minor (3)</td>
<td>Minor (2)</td>
<td>Minor (1)</td>
</tr>
<tr>
<td></td>
<td>Significant (10)</td>
<td>Significant (8)</td>
<td>Moderate (6)</td>
<td>Moderate (4)</td>
<td>Minor (2)</td>
</tr>
<tr>
<td></td>
<td>Major (15)</td>
<td>Significant (12)</td>
<td>Significant (9)</td>
<td>Moderate (6)</td>
<td>Minor (3)</td>
</tr>
<tr>
<td></td>
<td>Catastrophic (20)</td>
<td>Major (16)</td>
<td>Significant (12)</td>
<td>Significant (8)</td>
<td>Moderate (4)</td>
</tr>
<tr>
<td></td>
<td>Catastrophic (25)</td>
<td></td>
<td>Major (15)</td>
<td>Significant (10)</td>
<td>Moderate (5)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Severity</th>
<th>Minor (1)</th>
<th>Moderate (2)</th>
<th>Significant(3)</th>
<th>Major (4)</th>
<th>Catastrophic (5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(20-25)</td>
<td>Catastrophic and</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Major</td>
<td>Risk Treatment Strategies to be implemented by Directors/College Managers and action taken reported to the Risk Manager for consolidation and reporting to SMT.</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>(8-12)</td>
<td>Significant</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(4-6)</td>
<td>Moderate and Minor</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(1-3)</td>
<td>Minor</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Acceptable – to be managed under normal control procedures.
Appendix I: Legislation

Updated: 9 April 2018

- 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)
- Human Tissue Act 2008 (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 Act 1998 (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)
- Vulnerable Children Act 2014 (New Zealand Legislation website)
- Wages Protection Act 1983 (New Zealand Legislation website)
- Waitangi Day Act 1976 (New Zealand Legislation website)