## Document Control

<table>
<thead>
<tr>
<th>Version No.</th>
<th>Date</th>
<th>Revision Details</th>
<th>Author</th>
<th>Endorsed</th>
<th>Approved</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>27 April 2017</td>
<td>Draft for consultation</td>
<td>M. Cartwright</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>12 June 2017</td>
<td>Draft incorporating changes following consultation</td>
<td>M. Cartwright</td>
<td>VCAG</td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>23 June 2017</td>
<td>Final version</td>
<td>M. Cartwright</td>
<td>AudRiskComm</td>
<td></td>
</tr>
</tbody>
</table>
ACKNOWLEDGEMENTS

The Office of Audit, Risk and Assurance acknowledge those who created and implemented the existing Risk Management Framework, processes and tools at the University of Otago. These have created the foundation and context of this framework.

Further, the following resource documents have been relied on for development of this framework:

# CONTENTS

Acknowledgments

1. Purpose ......................................................................................................................... 5
2. Scope ............................................................................................................................. 6
3. Benefits ........................................................................................................................ 6
4. Risk Governance
   4.1 Risk Appetite ............................................................................................................. 6
   4.2 The Three Lines of Defence ..................................................................................... 7
   4.3 Audit & Risk Committee ......................................................................................... 8
   4.4 Risk Management Policy ......................................................................................... 8
5. The Risk Management Process
   5.1 Establish the Context ............................................................................................... 9
   5.2 Risk Identification ................................................................................................... 10
   5.3 Risk Analysis ........................................................................................................... 10
   5.4 Risk Evaluation ....................................................................................................... 13
   5.5 Risk Treatment ....................................................................................................... 13
   5.6 Communication and Consultation .......................................................................... 14
   5.7 Risk Monitoring and Control .................................................................................. 15
   5.8 Risk Management Process summary ...................................................................... 16
6. Related Assurance Frameworks and Plans
   6.1 Project Risk and Issues Management Framework ..................................................... 18
   6.2 Workplace Health & Safety .................................................................................... 18
   6.3 Legal Compliance Framework ................................................................................ 19
   6.4 Emergency Management Planning ......................................................................... 19
   6.5 Business Continuity Management .......................................................................... 19
   6.6 Disaster Recovery Planning .................................................................................... 19
   6.7 Internal and External Audit .................................................................................... 20
   6.8 Financial Management Assurance ........................................................................ 20
   6.9 Academic Quality Assurance ................................................................................ 21
   6.10 Annual Certification .............................................................................................. 21
7. Emerging Risks ............................................................................................................ 21
8. Training and Support .................................................................................................. 22
9. Roles and Responsibilities ............................................................................................ 22
10. Risk Escalation and Reporting
   10.1 Escalation ............................................................................................................... 22
   10.2 Reporting ............................................................................................................... 23
1. PURPOSE

The purpose of the Risk Management Framework is to provide the basis for the development and maintenance of a coordinated set of activities to respond to risks that may affect the ability of the University to achieve its mission and strategic objectives.

The framework outlines the plans, relationships, accountabilities, resources, processes, and activities that need to be undertaken to manage risk.

The framework is based on the Australia/New Zealand Risk Management Standard AS/NZS ISO 31000:2009 and establishes:

- A methodology for the identification, assessment and management of risk.
- Responsibilities for risk management across the University.
- Accountabilities for good governance.
- Mechanisms for the formal reporting of information relating to risk.

Key elements of the framework are summarised in the following diagram:

Figure 1: University of Otago – Risk Management Framework
RISK MANAGEMENT FRAMEWORK

2. SCOPE
This framework applies to all areas of the University’s business, including its academic, research, administrative, project and commercial activities. Entities are responsible for their own risk management activities and provide reports on the status of risk to the University’s Audit & Risk Committee annually and on the request of the Committee.

3. BENEFITS
The Risk Management Framework and associated activities:

- Link risk management to University planning processes – this provides a structured approach to the identification and management of risks that could impact on the University’s strategic and operational objectives.
- Improves the quality of decision making by providing methods and approaches for the exploration of threats and opportunities.
- Supports a culture of openness that encourages staff to identify risks and respond appropriately.
- Contributes to a robust and ethical culture of excellence in corporate governance.
- Provides assurances to the Vice-Chancellor and Council that critical risks are being managed.
- Helps to ensure that suppliers and contractors are aware of the University’s expectations regarding risk.

The principles upon which risk management are based are detailed in Appendix 1.

4. RISK GOVERNANCE
Risk governance refers to the culture and arrangements developed by the university to manage the risk to its mission and strategic objectives. It includes leadership, accountabilities and oversight and is an essential part of the University’s overall governance responsibilities.

Effective risk governance:
- Guides required risk management behaviours.
- Establishes consistent processes.
- Drives informed decision making.

The alignment of corporate and business planning to the Risk Management Framework is an essential component of good governance and provides value to decision makers as it will:
- Identify what could impact the University’s objectives.
- Provide an opportunity to develop strategies to minimise the impact.
- Support decisions on how much risk can be taken to achieve an objective.

4.1 Risk Appetite
The University’s risk appetite is the shared view of the Council, its Committees and the senior leadership team, and refers to the type and amount of risk that the University is prepared to accept or avoid to achieve its strategic objectives.
RISK MANAGEMENT FRAMEWORK

The risk appetite statement influences and guides decision making, clarifies strategic intent and helps to ensure choices align with the capacities and capabilities of the University.

In pursuing its vision, mission and strategic objectives the University will accept a level of risk proportionate to the expected benefits to be gained, and the impact or likelihood of damage.

The University has a high appetite for risk in the context of:
- Maintaining its reputation as a research-led university with international reach.
- Promoting critical thinking and intellectual independence.

The University has a low appetite for risk where there is a likelihood of:
- Significant reputational or financial damage.
- Harm to students, staff, collaborators or visitors.
- Illegal or unethical conduct or outcomes.

The University shall seek to formally identify and appropriately manage all potentially major and significant risks. Thresholds for identifying and managing less significant risks shall take account of the time and resources required for such activities.

The risk classification and rating tables that support the Risk Management Framework also provide guidance regarding the University’s appetite for risk (refer Appendix 3).

4.2 The Three Lines of Defence

The Three Lines of Defence Model is designed to ensure the effective and transparent management of risk by making accountabilities clear. Each of the three lines has a distinct role in the University’s governance and oversight. The Council, its Committees and senior management are the primary stakeholders that are served by the established lines and are in a position to ensure that the three lines of defence are reflected in the University’s risk management control processes.

- First line of defence - University Operations, academic and operational management has ownership, responsibility and accountability for directly assessing, controlling and mitigating risks.
- Second line of defence - consists of oversight and support functions such as Risk Management, Compliance, Quality, Finance.
- Third line of defence - Internal Audit, External Audit, regulators and other independent assurance providers who independently challenge both the first and second lines of defence.
4.3 Audit & Risk Committee

At each meeting of the Audit & Risk Committee, a high-level status report and commentary on risk management will be provided as part of standard reporting to the Committee.

In addition, risks assessed as high or very high will be reported to the Committee via the Corporate Risk Register. The Corporate Risk Register will include significant and aggregated risks drawn from subsidiary registers maintained for Divisions, Projects, Health & Safety, and Legal Compliance.

4.4 Risk Management Policy

The Risk Management Policy outlines the intent of the University with respect to risk management and describes governance arrangements and expectations. It provides guidance and helps to clarify expectations regarding attitude, awareness and accountabilities relating to risk management. A copy of the Risk Management Policy is located in the Policy Library on the University’s website.

5. THE RISK MANAGEMENT PROCESS

The risk management process is best summarised in the following diagram drawn from the Risk Management Standard AS/NZS ISO 31000:2009. The principles of risk management are incorporated into a framework that employs a structured process for the identification, treatment and communication of risk.

---

5.1 Establish the Context

The objectives, scope and parameters of the activity where the risk management process is to be applied, should be established. The context may vary according to the activity under review and may involve an evaluation of the following:

External Context
- The social, cultural, political, legal, regulatory, financial, technological, economic, natural, and competitive environment in which the activity occurs.
- Key drivers and trends.
- Stakeholder interests and perceptions.

Internal Context
- Strategic and/or operational objectives of the University and activity.
- University structure, culture, roles and responsibilities.
- Policies, procedures, and guidelines.

---

2 "Reproduced from Figure 1 of AS/NZ ISO 31000:2009 with the permission of standards NZ under copyright licence LN001223"
RISK MANAGEMENT FRAMEWORK

• Capabilities and resources.
• Information flows and decision-making processes (both formal and informal).
• Reports, surveys, questionnaires, business plans, audits, records or people that could provide expert judgement or knowledge.

5.2 Risk Identification

The aim of the risk identification process is to generate a comprehensive list of risks based on events that might enhance, prevent, accelerate or delay the achievement of strategic or operational objectives. The identification process should include all significant risks, regardless of whether or not the source of the risk is under the control of the University.

Where possible, include sources of quantitative or qualitative data in the identification process to assist in the analysis of the risk and the application of risk ratings i.e. past records, industry practice, knowledge experts, and performance indicators.

Common approaches to identifying risks include:

• Workshops
• Brainstorming sessions
• Benchmarking
• Questionnaires
• Interviews and meetings with stakeholders

When describing a risk, be specific and try to avoid broad statements and “types” of risk i.e. Health & Safety, Information Technology. These descriptions are less informative and may make the identification of controls and risk mitigations strategies difficult. In addition, remember that incidents or issues are not risks – they are risks that have materialised and treatment plans would focus on managing the incident or the issue itself (rather than on proactively preventing the incident or issue from occurring).

The broad categories of risk provided in Appendix 2 may assist with the identification and subsequent aggregation of risks.

5.3 Risk Analysis

Risk analysis and risk evaluation (refer part 5.4) are separate activities but are usually undertaken together.

Risk analysis involves developing a greater understanding of a risk and provides the basis upon which subsequent decisions regarding treatment options are made. The causes and sources of risk are considered together with the likelihood and impact of an event occurring.
Likelihood, Impact and Inherent Risk

The Risk Rating/Classification tables provided in Appendix 3 should be utilised to determine likelihood and impact scores.

The “likelihood” is an estimate of how likely the risk is to occur and is usually an approximate estimate only.

The “impact” or severity is an estimate of the effects of the risk if the risk eventuated.

Multiplying the likelihood score by the impact score provides the inherent risk rating/classification (refer Appendix 3).

**Example 1**

It is **Probable** that the University will experience a cyber-attack on its IT systems and if the student records system was unavailable for several days the impact would be **Severe**.

The inherent risk rating would therefore be 4 X 4 = 16 and the inherent risk classification “**Very High**”.

**Example 2**

If a fire started in a building on the Dunedin campus it is **Likely** that it could destroy the building and the impact on University services and operations would be **Serious**.

The inherent risk rating would therefore be 3 X 4 = 12 and the inherent risk classification “**High**”.

**Existing Controls**

The effectiveness of existing controls to mitigate risk is then assessed during this analysis. The best person to provide advice on controls is usually the risk owner, although specialist advice may be required depending on the nature of the risk.

To determine the quality of existing controls, look at what systems, procedures or practices currently exist to control the risk in question. Such controls may be management, technical, legal or procedural.

Examples of common controls include:

- Delegations
- Committees
- Reporting
- Policies, procedures and guidance material
RISK MANAGEMENT FRAMEWORK

- Qualifications
- Insurance
- Employment screening
- Training and required learning
- Position descriptions
- Code of conduct
- Reconciliations
- Segregation of duties
- Audits, reviews and investigations
- Checklists, templates
- Personal protective equipment
- Physical access controls
- IT firewalls
- Passwords
- Independent checks

Step 3 - Residual risk

After assessing the effectiveness of existing controls, the likelihood and/or impact ratings are adjusted to determine the level of residual risk.

A simple and reasonable approach is to consider whether the controls are:

- Effective and can be relied upon.
- Partially effective and can be relied upon in most circumstances.
- Ineffective and cannot be relied upon.

Example 1

It is Probable that the University will experience a cyber-attack on its IT systems and if student systems were unavailable for several days the impact would be Serious.

The inherent risk rating would therefore be 4 X 4 = 16 and the inherent risk classification “Very High”

IT Services however routinely scan key systems and applications for vulnerabilities and it has implemented password controls and firewalls. When these controls are considered, the likelihood is reduced and adjusted to Likely.

The residual risk rating would therefore be 3 X 4 = 12 and residual risk rating classification “High”.
Example 2

If a fire started in a building on the Dunedin campus it is Likely that it could destroy the building and the impact on University services and operations would be Serious.

The inherent risk rating would therefore be $3 \times 4 = 12$ and the inherent risk classification “High”.

The University however has installed fire detection, alarm and sprinkler systems in buildings on the Dunedin campus. When these controls are considered, the likelihood is reduced and adjusted to Rare.

The residual risk rating would therefore be $1 \times 4 = 4$ and residual risk rating classification “Low”.

The level of detail produced during the analysis phase may vary, depending on the risk and the purpose of the analysis. The analysis can also be qualitative or quantitative and should involve key stakeholders and knowledge experts where appropriate.

5.4 Risk Evaluation

The purpose of risk evaluation is to assess what risks require treatment and in what order of priority. Decisions should be made in accordance with legal and regulatory requirements and include a consideration of available resourcing and the University’s appetite for risk, particularly in terms of potential financial and reputational impact.

Risk evaluation should also take into account the degree of control over each risk and the cost impact, benefits and opportunities presented by the risk.

5.5 Risk Treatment

Risk treatment involves selecting one or more options for modifying risks, and implementing those options.

Options for treating risks are not mutually exclusive and may include the following approaches:

- **Avoid** – do not start or continue with the activity that gives rise to the risk.
- **Transfer** or share risk – through contracts, partnerships, risk financing, insurance etc.
- **Reduce** – implement controls and other treatments to reduce the impact or likelihood of an event.
- **Accept** – retain the risk by informed decision and develop a contingency plan if appropriate to minimise the impacts should they arise.
The following questions may also help to decide the options to treat risks:

- What is the feasibility of each treatment option?
- What is the cost of implementing versus the benefits?
- What is the extent of risk treatment versus the benefits?
- What are the resources needed (staff, funds, technical)?
- Do the risk treatments comply with legal requirements, government and organisational policies including those concerning access, equity, ethics and accountability?
- What opportunities are created by the risk?

After careful consideration, risk treatments may also involve decisions to take or increase the risk in order to pursue an opportunity for the University.

The most appropriate treatment option involves balancing costs against benefits together with due regard to legal, regulatory and other requirements such as social responsibility, the mission and the strategic objectives of the University and the safety of staff and students.

If, after treatment, there remains an unacceptably high residual risk, a decision should be taken about whether to retain this risk, repeat the risk treatment process, or continue to monitor and review the risk.

The actions required based on the residual risk ratings can also be found in the Risk Rating/Classification table in Appendix 3.

**Risk Treatment Plans**

For significant risk issues it may be appropriate to develop a detailed risk treatment plan that outlines the treatment options and the priority in which they will be implemented. The plans should ideally include:

- Proposed treatment actions.
- Responsibilities for approving the plan and implementing the plan.
- Resourcing requirements.
- Reporting and monitoring requirements.
- Timeframes for completion including the frequency of review of the treatment plan.

Where possible treatment options should be embedded into existing day-to-day practices or processes.

**Contingency Plans**

A contingency plan is an action or set of activities that will be implemented once a trigger is reached and it is used to help manage a risk as it shifts towards being an issue. A trigger may be an event, a threshold, a date or other item that indicates that it is time to put backup plans into action.
Contingency plans may be developed for risks that are unlikely or rare but if realised, would have a catastrophic impact on the University, a project or the health and safety of staff, students or contractors.

The plans should ideally include:

- Trigger, timeline and actions.
- Realistic goals/objectives and the purpose of the plan.
- Actions and proposed responses.
- Responsibilities of nominated staff.

5.6 Communication and Consultation

Communication and consultation with internal and external stakeholders should take place at all stages of the risk management process and plans to communicate risks, causes, impacts, and treatments should be developed. This will help to:

- Ensure the interests of stakeholders are understood.
- Bring different areas of expertise together to better analyse risk and reduce uncertainty.
- Assist with the development of risk criteria.
- Secure endorsement and support for the treatment of risk.

Stakeholders are people who are (or perceive themselves to be) directly affected by a decision or activity and can supply essential information and valuable feedback during the risk analysis process.

Stakeholders are likely to make judgments about risk based on their perceptions. These can vary due to differences in values, needs, assumptions and concerns as they relate to the risks or the issues under discussion. Since the views of stakeholders can have a significant impact on the decisions made, it is important to identify and document their differing perception of risks and benefits.

Communications Plan

A Communications Plan can be used to ensure that:

- All stakeholders have been identified.
- Consistent messages are sent to relevant stakeholder groups.
- Risk messages are sent out at times and with a frequency that supports business objectives and follows business planning cycles.

The template provided in Appendix 4 can be used to develop a communication approach. The plan should link to the risk mitigation strategies and provide a summary of key risk management communications planned over a period, typically 1 year.
Communications could include:

- Regular reports on the status of the risk management process for the Council, Audit & Risk Committee, senior management.
- Reports to Project Teams and other stakeholders identified when establishing the context (the first step in the risk management process).
- Invitations to periodic risk assessment workshops/meetings.
- Articles to be included in staff newsletters, intranet etc.
- Risk management progress reports included in annual reports.

5.7 Risk Monitoring and Control

Monitoring and review is an essential and ongoing component of the risk process and is undertaken in order to:

- Detect any changes in the internal or external context.
- Identify emerging risks.
- Assess the performance of treatment options.
- Assess if a risk has changed and requires escalation, or is no longer valid and can be archived.

The reviews may be self-initiated or undertaken by independent assessors such as internal or external auditors.

Ideally, active risks should be a standing item on Divisional, Departmental, Corporate and Committee/Council meeting agendas.
### 5.8 Risk Management Process Summary

<table>
<thead>
<tr>
<th>Process Step</th>
<th>Step Summary</th>
<th>Tools &amp; Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Establish the Context</td>
<td>• Operational or Strategic Plans</td>
</tr>
<tr>
<td>Establish the</td>
<td>• Establish the external, internal and risk management context in which the</td>
<td>• Financial data</td>
</tr>
<tr>
<td>Context</td>
<td>rest of the process will take place. Reference risk categories, such as,</td>
<td>• Stakeholder input</td>
</tr>
<tr>
<td></td>
<td>legal or regulatory requirements and the objectives to be achieved.</td>
<td>• Subject matter experts</td>
</tr>
<tr>
<td></td>
<td>• Operational or Strategic Plans</td>
<td>• Workshops</td>
</tr>
<tr>
<td></td>
<td>• Financial data</td>
<td>• Risk Categories</td>
</tr>
<tr>
<td></td>
<td>• Stakeholder input</td>
<td>• Risk Categories</td>
</tr>
<tr>
<td></td>
<td>• Subject matter experts</td>
<td>• Risk Categories</td>
</tr>
<tr>
<td></td>
<td>• Workshops</td>
<td>• Risk Categories</td>
</tr>
<tr>
<td>Step 2</td>
<td>Risk Identification</td>
<td>• Risk categories</td>
</tr>
<tr>
<td></td>
<td>• Identify where, when, why and how events could prevent, delay or enhance</td>
<td>• Reports, audits and reviews</td>
</tr>
<tr>
<td></td>
<td>the achievement of operational or strategic objectives.</td>
<td>• Historical data/trends</td>
</tr>
<tr>
<td></td>
<td>• Risk categories</td>
<td>• Stakeholder input</td>
</tr>
<tr>
<td></td>
<td>• Reports, audits and reviews</td>
<td>• Subject matter experts</td>
</tr>
<tr>
<td></td>
<td>• Historical data/trends</td>
<td>• Workshops</td>
</tr>
<tr>
<td></td>
<td>• Stakeholder input</td>
<td>• Workshops</td>
</tr>
<tr>
<td></td>
<td>• Subject matter experts</td>
<td>• Workshops</td>
</tr>
<tr>
<td></td>
<td>• Workshops</td>
<td>• Workshops</td>
</tr>
<tr>
<td>Step 3</td>
<td>Risk Analysis</td>
<td>• Cost/benefit assessments</td>
</tr>
<tr>
<td></td>
<td>• Analyse identified risks to determine the level of inherent risk.</td>
<td>• Risk appetite statement</td>
</tr>
<tr>
<td></td>
<td>• Identify and evaluate existing controls.</td>
<td>• Risk Categories</td>
</tr>
<tr>
<td></td>
<td>• Revise likelihood and impact ratings to gauge the level of residual risk.</td>
<td>• Risk Categories</td>
</tr>
<tr>
<td></td>
<td>• Risk Classification Table</td>
<td>• Risk Categories</td>
</tr>
<tr>
<td></td>
<td>• Risk Matrix</td>
<td>• Risk Categories</td>
</tr>
<tr>
<td>Step 4</td>
<td>Risk Evaluation</td>
<td>• Cost/benefit assessments</td>
</tr>
<tr>
<td></td>
<td>• Evaluate risks by comparing the level of risk found during the risk analysis</td>
<td>• Risk appetite statement</td>
</tr>
<tr>
<td></td>
<td>process with the risk categories established.</td>
<td>• Risk Categories</td>
</tr>
<tr>
<td></td>
<td>• Consider resources required to address or pursue risk.</td>
<td>• Risk Categories</td>
</tr>
<tr>
<td></td>
<td>• Risk Register</td>
<td>• Risk Categories</td>
</tr>
<tr>
<td></td>
<td>• Risk Treatment Plan</td>
<td>• Risk Categories</td>
</tr>
<tr>
<td></td>
<td>• Contingency Plan</td>
<td>• Risk Categories</td>
</tr>
<tr>
<td>Step 5</td>
<td>Risk Treatment</td>
<td>• Stakeholders</td>
</tr>
<tr>
<td></td>
<td>• Develop and implement specific strategies/controls and action plans to</td>
<td>• Communications Plan</td>
</tr>
<tr>
<td></td>
<td>mitigate/pursue risk.</td>
<td>• Workshops</td>
</tr>
<tr>
<td></td>
<td>• Risk Register</td>
<td>• Interviews</td>
</tr>
<tr>
<td></td>
<td>• Risk Treatment Plan</td>
<td>• Risk Registers</td>
</tr>
<tr>
<td>Steps 6</td>
<td>Communicate and Consult</td>
<td>• Stakeholders</td>
</tr>
<tr>
<td></td>
<td>Continual Process: Monitor and review the effectiveness of all steps taken</td>
<td>• Communications Plan</td>
</tr>
<tr>
<td></td>
<td>in the risk management process. Communicate and consult with internal and</td>
<td>• Workshops</td>
</tr>
<tr>
<td></td>
<td>external stakeholders.</td>
<td>• Interviews</td>
</tr>
<tr>
<td></td>
<td>• Stakeholders</td>
<td>• Reports, audits and reviews</td>
</tr>
<tr>
<td></td>
<td>• Communications Plan</td>
<td>• Risk Registers</td>
</tr>
<tr>
<td></td>
<td>• Workshops</td>
<td>• Risk Registers</td>
</tr>
<tr>
<td>Steps 7</td>
<td>Monitor and Review</td>
<td>• Stakeholders</td>
</tr>
<tr>
<td></td>
<td>Continual Process: Monitor and review the effectiveness of all steps taken</td>
<td>• Communications Plan</td>
</tr>
<tr>
<td></td>
<td>in the risk management process. Monitor, record and report on risks and the</td>
<td>• Workshops</td>
</tr>
<tr>
<td></td>
<td>effectiveness of treatment measures to ensure that changing circumstances do</td>
<td>• Interviews</td>
</tr>
<tr>
<td></td>
<td>not alter priorities.</td>
<td>• Reports, audits and reviews</td>
</tr>
<tr>
<td></td>
<td>• Reports, audits and reviews</td>
<td>• Risk Registers</td>
</tr>
</tbody>
</table>
RISK MANAGEMENT FRAMEWORK

6. RELATED ASSURANCE FRAMEWORKS AND PLANS

The Risk Management Framework is the means by which intelligence regarding risk across the entire University is identified and aggregated. This information is used to support the achievement of the University’s mission and strategic objectives by proactively responding to threats and providing an additional source of guidance when pursuing opportunities. There are a number of key frameworks and activities at the University that identify and respond to risk that support the development and implementation of the University’s framework:

6.1 Project Risk and Issues Management Framework

This Project Risk and Issues Management Framework has been designed to ensure the University has an effective system in place to manage risks within the project environment.

The framework provides a management tool to project participants conducting projects on behalf of the University. It has the following goals that align with the University Risk Management Framework:

- Facilitate the achievement of the University’s strategic and project goals by managing risks that could otherwise create barriers.
- Apply risk management practices as part of long term and day-to-day project planning and decision making.
- Develop a culture of openness that encourages project participants to quickly identify risks and to respond appropriately.
- Facilitate continual improvement of University project activities.
- Create a robust and ethical culture of excellence in corporate and project governance.
- Provide assurance to the Vice-Chancellor, Council and the Project Steering Committees that critical risks are being managed effectively.

A Risk Register is maintained for each major project. A copy of the most current framework can be obtained from the Project Management Office.

6.2 Workplace Health & Safety

The University of Otago is committed to providing a safe and healthy workplace for workers, students and visitors. Accordingly, the University actively seeks to comply with the relevant Workplace Health and Safety legislation, codes of practice, guidelines, and standards.

The health and safety management structure supports and facilitates the development of health and safety policies, risk registers, risk control strategies, hazard management processes, defines responsibilities, and ensures open communication on health and safety issues.
The University also maintains an online Health and Safety management system (Vault). The system allows all staff, students, contractors and visitors to the University campuses to report any health and safety related event on site.

Further information regarding workplace health and safety management systems can be accessed on the University’s website or by contacting the Office of Health and Safety Compliance.

### 6.3 Legal Compliance Framework

A Legal Compliance Framework is currently under development, further information can be obtained from the Office of Risk, Assurance and Compliance.

### 6.4 Emergency Management Planning

The Emergency Management Plan sets out the arrangements for a co-ordinated action by the University in response to an emergency on campus.

These emergencies cover a very wide field of possible events that include:

- Natural disasters such as flooding, earthquake, or storms.
- Hazardous substance, leaks, or spills.
- Terrorism.
- Violence.
- Criminal activity and unrest.

The University’s main objectives in its initial response to all emergencies are:

- To protect human life and alleviate suffering, and, as far as possible, protect property and reputation.
- To support the continuity of everyday activity and the restoration of disrupted services at the earliest possible time.

The Emergency Management Plan supports these objectives by providing a clear and organised response strategy supported by pre-defined response procedures.

Further information regarding emergency management planning can be accessed on the University’s website or by contacting the Proctor’s Office, Student Services.

### 6.5 Business Continuity Management

The University’s Business Continuity Management Framework is currently undergoing revisions, further information can be obtained from the Office of Risk, Assurance and Compliance.

### 6.6 Disaster Recovery Planning

The Disaster Recovery Plan provides guidance on how to respond to Information Technology Services disasters where critical information technology services are physically damaged due to fire, flood,
electricital failure, sabotage by personnel, malicious attack or some other harmful event. The Plan is designed to help ensure the University is able to:

- Ensure the availability of services.
- Minimise loss and facilitate recovery of core IT infrastructure assets.
- Preserve the University of Otago’s public image and reputation within the community.
- Prevent the disaster from threatening the University of Otago’s long term stability and viability.
- Heighten organisational awareness, allow for advanced preparation and workforce education and training.

For further information regarding Disaster Recovery Planning contact Information Technology Services.

6.7 Internal and External Audit

University management is responsible for ensuring that satisfactory systems of internal control are in place to ensure that the financial information produced is reliable, that University assets are safeguarded and that the University resources are used efficiently and effectively.

One of the mechanisms for ensuring that these objectives are achieved is the establishment of an independent Internal Audit function. The Internal Audit function reviews accounting records, management information systems and other administrative policies and practices throughout the University and reports outcomes to the Audit & Risk Committee. The role includes the identification and recommendation of measures to achieve greater effectiveness, efficiency and economy. It also assesses non-compliance with policies or regulatory requirements and contribute to measures to prevent fraud and corruption.

The integrity of internal controls is also routinely assessed by the University’s external auditors when undertaking financial statement audits.

6.8 Financial Management Assurance

The Financial Services Division contributes to the mitigation of financial risks through its maintenance of financial planning, performance and reporting systems. Significant strategic and operational matters relating to budgets, business cases and forecasting are managed by its financial and management accounting functions. The Finance Office also:

- Mitigates risk associated with procurement.
- Prepares the annual financial statements.
- Reviews the University’s insurance strategy on an annual basis, taking into account the risk profile, the prevailing status of the insurance market and the University’s risk appetite.
6.9 Academic Quality Assurance

The Quality Assurance Unit undertakes a cyclical program of reviews designed to assess and improve the University’s teaching and research. Policies and systems for assuring quality are also evaluated and risks to strategic positioning, operations, resourcing, teaching, research and services are assessed. Further information regarding this program can be obtained from the Quality Advancement Unit.

6.10 Annual Certification

At the end of each financial year the Chancellor and Vice-Chancellor sign a Statement of Responsibility contained in the University of Otago Financial Statements whereby they accept responsibility for establishing and maintaining a system of internal control designed to provide reasonable assurance as to the integrity and reliability of the financial reporting.

When accepting this responsibility, the Vice-Chancellor places reliance on a range of key administrative and financial controls across the University.

The Annual Certification process supports this sign-off by recognising and evaluating the wider accountabilities for internal financial controls and compliance that exist across all University of Otago operations. It involves a self-assessment of controls by key financial delegation holders within the context of a risk-based internal control framework widely adopted in North America known as COSO (after the name of the organisation that developed it - Committee of Sponsoring Organizations of the Treadway Commission).

The annual certification will be facilitated by the Office of Risk, Assurance and Compliance in close co-operation with the Financial Services Division.

7. EMERGING RISKS

In order to identify unwelcome trends and emerging risks, the University will develop and maintain a Risk Data Management (RDM) system. The database will be populated with information arising from incidents and near miss events that are routinely reported from across all areas of the University i.e.

- Workplace Health & Safety - reportable incidents and aggregated data (Vault system).
- Key Risk Indicators – metrics established when significant risks are first identified or when the negative impact of a risk significantly increases.
- Services - complaints and issues reported from both internal and external sources.
- Learning from Adverse Events - the outcomes of investigations, audits, reviews and organisational learning processes.
- Governance - in the course of their business it is anticipated that the various Council Committees and controlled entities will identify risk.
- Data analysis – other metrics relating to performance, workforce, finance and quality extracted from major corporate IT systems (Finance, Human Resource, Students).

This data will be aggregated and reviewed by the Office of Audit, Risk Assurance and the outcomes used to co-ordinate a proactive response to emerging risk.
8. TRAINING AND SUPPORT

To ensure that adequate risk management competency levels are achieved and maintained, the University will provide regular training courses in the risk management process and its application in the University.

Specific risk management training sessions will also be held with Divisions on a regular basis, aimed at providing an overview of the Risk Management Framework. The training will be facilitated by the Office of Risk, Assurance and Compliance. Additional ad-hoc training will also be provided as required/on request.

9. ROLES AND RESPONSIBILITIES

The roles and responsibilities of the Council, Audit and Risk Committee and staff are detailed in the Risk Management Policy which can be accessed on the University website. Additional roles include:

Internal Audit
- Undertakes regular independent reviews of the adequacy and effectiveness of the Risk Management Framework and related risk management processes.
- Reports outcomes to the Audit & Risk Committee.

Risk Owner
- Monitors the status of their assigned risks.
- Advises the owner of the Risk register on the appropriateness of responses to the risk and control measures.
- Confirms that control and risk mitigation measures are in place and working effectively.

Action Owners
- Inform the relevant Risk Owner of any issues relating to the implementation of assigned actions.
- Manages and allocates resources to ensure that the mitigating actions they are responsible for are undertaken and completed within the time frame specified.
- Updates their assigned risks in the Risk Register located in OURDrive when they occur or at the time of quarterly reporting to the Audit & Risk Committee.

10. RISK ESCALATION AND REPORTING

10.1 Escalation

Risks recorded in the subsidiary Risk Registers maintained for Divisions, Project Management, Legal and Health & Safety may be escalated and included in the Corporate Risk Register. This will occur if the risk represents an issue that has the potential to hinder achievement of the strategic objectives detailed in the “Strategic Direction to 2020” plan and the underlying activities (as expressed in the “SD2020 Action Plan”). The decision to escalate a risk will invariably be based on professional
judgement. However, if there is any uncertainty staff are encouraged to refer the matter to their senior manager, Director of Risk, Assurance & Compliance or the Chief Operating Officer.

The Office of Risk, Assurance and Compliance also reviews High and Very High risks in subsidiary risk registers with a view to escalation where:

- There has been a significant adverse change in the status of a significant risk.
- To reflect the aggregated significance of similar risks presenting on several risk registers.

### 10.2 Reporting

The Subsidiary and Corporate Risk Registers should be regularly reviewed and updated, ideally on at least a monthly basis. A full review will be undertaken on a quarterly basis and outcomes will form part of progress reports to the Audit & Risk Committee. Reporting deadlines will be communicated to staff at the commencement of each calendar year.

Reports to the Audit & Risk Committee will include:

- All High and Very High corporate risks.
- An executive summary of significant changes in the University risk profile.
- Commentary on significant residual risks and associated mitigation efforts.

Reports will also include profiling charts and risk assurance maps when implementation of the Risk Management Framework has been sufficiently advanced (refer Appendix 6). These charts can also be adapted to report on the status of risk recorded in subsidiary risk registers.

### 10.3 Closing of Risks

The Risk Owner may close risks when remedial actions are complete and the predetermined target risk rating has been achieved. The Audit & Risk Committee is to be formally notified when closing High and Very High risks maintained in the Corporate Risk Register. This notification will form part of regular risk reports to the Committee at each Committee meeting.

### 10.4 Risk Registers

The Risk Registers are located in OURDrive which is accessible from the University’s website and instructions for accessing the Registers can be obtained from the Office of Risk, Assurance and Compliance. The system also provides risk reports based on standardised templates.

The registers have been designed to capture risks, facilitate an enterprise-wide response to risk and provide a means for recording risks and the active mitigation of risk.

Access to OURDrive is controlled and, whilst the information it contains is not strictly confidential, it is for internal use only and access should be on a needs-to-know basis only.

Please note that workplace health and safety issues should still be reported separately in accordance with the University’s Health & Safety Policy and as provided for on the Health and Safety Web Portal. The Office of Health & Safety Compliance will in turn determine which health and safety issues will be escalated from its system (Vault) to the Corporate Risk Register.
With the exception of workplace health and safety, all Divisions are required to maintain registers on OURDrive – any exceptions should be communicated to the Office of Risk, Assurance and Compliance.

11. CONTACT INFORMATION

For further information regarding the Risk Management Framework contact the Office of Audit & Risk Assessment on 03 479 5970 or email risk.management@otago.ac.nz
GLOSSARY OF TERMS

Context - the internal and external environment that is considered when commencing a risk assessment, it helps define the scope of activities and is used to define risk criteria.

Controls - the measures that modify or reduce risk. Controls include any process, policy, device, practice or other action that minimises negative risks or contains them to an acceptable level.

Corporate Risks - those that may have a major impact on the strategic objectives of the University in the delivery of its objectives or the achievement of performance measures. Corporate risks are listed in the Corporate Risk Register, which is the responsibility of the Chief Operating Officer (under delegated authority from the Vice-Chancellor).

Divisional Risks - those which would seriously inhibit the achievement of the aims and objectives of a Division. They differ from Corporate risks in that their impacts would affect only one Division, rather than spanning across a number of Divisions. Divisional risks are managed by the Head of Division and listed in the Divisional Risk Register.

Governance - the framework by which an organisation is directed and controlled.

Issue - an event that has happened or which has a high likelihood of happening that may impede the achievement of objectives if not resolved. Issues are not risks.

Inherent 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.

Impact (or consequence) - the outcome of an event which impact objectives 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.

OURDrive - the University of Otago’s electronic document and records management system.

Residual Risk - the risk remaining after risk treatment/application of controls.

Risk - an uncertain event or condition that, if it occurs, has a positive or negative effect on objectives. It is often expressed in terms of a combination of the impact of an event and the associated likelihood of occurrence.

Risk Appetite - the amount and type of risk that an organisation is willing to pursue or retain.

Risk Assessment - the overall process of identifying, analysing, and evaluating risks. It may also be referred to as ‘risk profiling’ and may involve a qualitative and/or quantitative assessment.

Risk Attitude - refers to the University’s approach to assess and eventually pursue, retain, take, or turn away from risk.

Risk Management - coordinated activities to direct and control an organisation with regard to risk.

Risk Management Framework - the set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation.
**Risk Management Framework**

**Risk Matrix** - a tool for ranking and displaying risks by defining ranges for impacts and likelihood.

**Risk Owner** - the person or entity with the accountability and authority to manage a risk.

All risks in the risk register are ‘owned’ by a single named individual on the understanding that it may take shared responsibility to mitigate the risk successfully. Ownership of corporate risks is assigned by the Chief Operating Officer. Ownership of Divisional risks is assigned by the Head of Division.

**Risk Profile** - description of any set of risks. It is a structured approach to the identification and assessment of risk. The output of the risk identification and assessment process is a completed risk profile i.e. a Risk Register or in a graphical/chart format.

**Risk Register** - a document containing the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning. The register includes identified risks, descriptions, category, cause, likelihood of occurring, impact on objectives, mitigation strategies, owners, and status. The risk register facilitates standardised reporting of risks within the approved University governance framework.

**Stakeholder** - a person or organisation that can affect, be affected by or perceive themselves to be affected by a decision or activity.

Note: Definitions are in some instances, paraphrased from the Joint Australian New Zealand International Standard Risk Management, pp 2-5 [AS/NZS ISO 31000:2009].
Appendices:

1. Risk Management Principles
2. Categories of Risk
3. Risk Rating/Classification Table
4. Communication Plan Template
5. Risk Register Data Entry Screen - OURDrive
6. Risk Profiles and Assurance Mapping
Appendix 1

Risk Management Principles:
The principles of risk management are that risk management:

- Creates and protects value
  - Contributes to the achievement of objectives
  - Assists to improve performance

- Is an integral part of planning and management processes
  - Integrated into strategic and business planning
  - Guides prioritisation and clarifies responsibilities

- Is part of decision making
  - Explicitly incorporated into projects, system design and resource allocation.
  - Distinguishes among alternative courses of action.

- Explicitly addresses uncertainty
  - Identifies vulnerabilities
  - Promotes a shared view of risks and risk appetite

- Is systematic, structured, and timely
  - Facilitates comparability of results and benchmarking
  - Contributes to a consistent and efficient approach

- Is based on the best available information
  - Specifies the functional requirements of risk management systems
  - Provides stakeholders with accurate and reliable data

- Risk Management is tailored
  - Designed and operated to fit with the University’s context and capabilities
  - Complies with legal obligations and adequate resources are allocated

- Takes human and cultural factors into account
  - Considers how people and culture interact with its functions
  - Monitors risk culture and behaviour

- Is transparent and inclusive
  - Identifies scope and method for risk monitoring and reporting to stakeholders
  - Identifies the role of stakeholders in the risk management process

- Is dynamic, iterative and responsive to change
  - Ensures strategy takes into account emerging risks
  - Ensures the Risk Management Framework is responsive to changes in context

- Facilitates continual improvement
  - Risk attestation and the results of internal and external audit are used to inform continual improvement
  - Stakeholder feedback is sought to influence the ongoing development of the Risk Management Framework

(Source: AS/NZS ISO 31000:2009)
<table>
<thead>
<tr>
<th>Risk Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Environmental</strong></td>
<td>• Security&lt;br&gt;• Waste management</td>
</tr>
<tr>
<td><strong>External Relations &amp; Partnerships</strong></td>
<td>• Collaborative teaching and research with other institutions/associations</td>
</tr>
<tr>
<td><strong>Financial and Economic</strong></td>
<td>• Sustainability of income streams&lt;br&gt;• Budget management/Forecasting&lt;br&gt;• Investments&lt;br&gt;• Financial processes/systems&lt;br&gt;• Procurement</td>
</tr>
<tr>
<td><strong>Learning, Teaching and the Student Experience</strong></td>
<td>• Academic Standards&lt;br&gt;• Student recruitment/numbers&lt;br&gt;• Courses and programmes (relevance and quality)&lt;br&gt;• Teaching quality and academic freedom&lt;br&gt;• The student experience (quality of Student Services, Accommodation)</td>
</tr>
<tr>
<td><strong>Organisational Management</strong></td>
<td>• Insurance&lt;br&gt;• Contract Approvals&lt;br&gt;• Public Liability&lt;br&gt;• Legal Relationships (breach of contract)&lt;br&gt;• Legal and policy compliance&lt;br&gt;• Projects (management and contractor performance)</td>
</tr>
<tr>
<td><strong>Property and Facilities</strong></td>
<td>• Property &amp; Physical Asset Mgmt.&lt;br&gt;• Sustainability&lt;br&gt;• Fleet&lt;br&gt;• Quality/availability of property and infrastructure-impact on students/staff</td>
</tr>
<tr>
<td><strong>Research &amp; Enterprise</strong></td>
<td>• Performance Based Research Fund&lt;br&gt;• Clinical Trials&lt;br&gt;• Ethical research issues&lt;br&gt;• Research funding &amp; grant mgmt.</td>
</tr>
<tr>
<td><strong>Service Quality</strong></td>
<td>• Quality and efficiency of administrative processes/services</td>
</tr>
<tr>
<td><strong>Staffing and Human Resources</strong></td>
<td>• Staff Mgmt. /Performance Mgmt.&lt;br&gt;• Staff recruitment and retention&lt;br&gt;• Succession planning/staff turnover&lt;br&gt;• Training &amp; Development&lt;br&gt;• Industrial Action&lt;br&gt;• Conflicts of Interest</td>
</tr>
<tr>
<td><strong>Workplace Health and Safety</strong></td>
<td>• Asbestos&lt;br&gt;• Unsafe work environment&lt;br&gt;• Slips, trips and falls</td>
</tr>
<tr>
<td>Overall Risk (L X I)</td>
<td>Likelihood (L)</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------</td>
</tr>
<tr>
<td><strong>Very High</strong></td>
<td>(5) Almost Certain</td>
</tr>
<tr>
<td></td>
<td>• Will undoubtedly happen</td>
</tr>
<tr>
<td></td>
<td>• Greater than 80% chance</td>
</tr>
<tr>
<td></td>
<td><strong>High</strong></td>
</tr>
<tr>
<td></td>
<td>(10 – 14)</td>
</tr>
<tr>
<td></td>
<td>• Will probably happen</td>
</tr>
<tr>
<td></td>
<td>• 50 - 80% chance</td>
</tr>
<tr>
<td></td>
<td><strong>Medium</strong></td>
</tr>
<tr>
<td></td>
<td>(5 – 9)</td>
</tr>
<tr>
<td></td>
<td>• Might happen</td>
</tr>
<tr>
<td></td>
<td>• 20 - 50% chance</td>
</tr>
<tr>
<td></td>
<td><strong>Low</strong></td>
</tr>
<tr>
<td></td>
<td>(3 - 4)</td>
</tr>
<tr>
<td></td>
<td>• Not expected to happen</td>
</tr>
<tr>
<td></td>
<td>• 5 - 20% chance</td>
</tr>
<tr>
<td></td>
<td><strong>1 - 2</strong></td>
</tr>
<tr>
<td></td>
<td>• Less than 5% chance</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Overall Risk</td>
<td>Likelihood (L)</td>
</tr>
<tr>
<td>-------------</td>
<td>--------------</td>
</tr>
</tbody>
</table>
| **Very High** > 15 | (5) Almost Certain | (5) Very Serious | Life threatening:  
  - Loss of life(s)  
  - Major health and safety incident involving staff or members of the public  
  - Permanent disability  
  - Permanent ill-health |
| **High** 10 - 14 | (4) Probable | (4) Serious | Extensive injuries:  
  - Loss of life  
  - Significant health and safety incident involving staff or members of the public  
  - Multiple serious injuries  
  - Long term illness/disability |
| **Medium** 5 - 9 | (3) Likely | (3) Moderate | Minor injuries:  
  - Possible hospitalisation  
  - Numerous days lost  
  - Short term illness |
| **Low** 3 - 4 | (2) Unlikely | (2) Minor | Potential for injury:  
  - Medical/ First Aid treatment required  
  - Some days lost |
| **Near Miss** 1 - 2 | (1) Rare | (1) Negligible | No injuries:  
  - Report, record and review. |

<table>
<thead>
<tr>
<th>Overall Risk</th>
<th>Likelihood (L)</th>
<th>Impact (I)</th>
<th>Project Management</th>
</tr>
</thead>
</table>
| **Very High** > 15 | (5) Almost Certain | (5) Very Serious | Detrimental impact on operations or major projects:  
  - Capital cost impact – *specific to project*  
  - Recurrent cost impact exceeds $5,000,000  
  - 3 months slippage  
  - Catastrophic impact on project objectives, identified benefits, deliverables  
  - Multiple irreversible injuries/illness or multiple fatalities |
| **High** 10 - 14 | (4) Probable | (4) Serious | Major impact on operations or major projects:  
  - 1 Capital cost impact – *specific to project*  
  - Recurrent cost impact exceeds $1,500,000  
  - 2 months slippage  
  - Significant impact on project objectives, identified benefits, deliverables  
  - Irreversible injury/illness, permanent disability or fatality |
| **Medium** 5 - 9 | (3) Likely | (3) Moderate | Moderate impact on operations or major projects:  
  - Capital cost impact – *specific to project*  
  - Recurrent cost impact exceeds $300,000  
  - 1 month slippage  
  - Some impact on project objectives, identified benefits, deliverables  
  - Serious injury/illness – lost time of more than 4 days |
| **Low** 3 - 4 | (2) Unlikely | (2) Minor | Minor impact on operations or major projects:  
  - 1 Capital cost impact – *specific to project*  
  - Recurrent cost impact exceeds $75,000  
  - 2 weeks slippage,  
  - Small impact on project objectives, identified benefits, deliverables  
  - Injury/ illness – lost time of less than 4 days |
| **Near Miss** 1 - 2 | (1) Rare | (1) Negligible |  
  - Capital cost impact – *specific to project*  
  - Recurrent cost impact less than $75,000 |
## Communications Plan Template

<table>
<thead>
<tr>
<th>Stakeholders/ Target Audience</th>
<th>Purpose/ Objective of Communication</th>
<th>Key Message/ Content</th>
<th>Communication Channel/ Method</th>
<th>Timing/ Date</th>
<th>Frequency</th>
<th>Communication Prepared By</th>
<th>Communication Approved By</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Internal:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Council</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vice-Chancellor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Project Team/s</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All Staff</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specific Departments/Divisions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>External:</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Clients</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Partners /Suppliers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other Institutions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Risk Register Data Entry Screen – OURDrive

#### Risk Details

<table>
<thead>
<tr>
<th>Risk Title*</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Objectives Potentially Impacted*</th>
<th>New field, not yet implemented - Reference the strategic, operational or project plan potentially impacted by this risk.</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Description of Cause*</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Risk Categories</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Environmental</td>
<td></td>
</tr>
<tr>
<td>External Relations and Partnerships</td>
<td></td>
</tr>
<tr>
<td>Financial and Economic</td>
<td></td>
</tr>
<tr>
<td>Learning Teaching and the Student Experience</td>
<td></td>
</tr>
<tr>
<td>Organisational Management</td>
<td></td>
</tr>
<tr>
<td>Property and Facilities</td>
<td></td>
</tr>
<tr>
<td>Research and Enterprise</td>
<td></td>
</tr>
<tr>
<td>Service Quality</td>
<td></td>
</tr>
<tr>
<td>Staffing and Human Resources</td>
<td></td>
</tr>
<tr>
<td>Workplace Health and Safety</td>
<td></td>
</tr>
</tbody>
</table>

Choose which categories this risk applies to.

<table>
<thead>
<tr>
<th>Risk Owner*</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter a name or email address …</td>
<td></td>
</tr>
</tbody>
</table>

#### Control Environment

<table>
<thead>
<tr>
<th>Inherent Risk Likelihood*</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The likelihood of an activity if no controls or other mitigating factors were in place (the gross risk or risk before controls)

<table>
<thead>
<tr>
<th>Inherent Risk Impact*</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The impact of an activity if no controls or other mitigating factors were in place (the gross risk or risk before controls)

Controls in Place and Working*

Residual Risk Likelihood*
The likelihood that remains after controls are taken into account (the net risk or risk after controls)

Residual Risk Impact*
The impact that remains after controls are taken into account (the net risk or risk after controls)

Control Environment

Further actions to be taken to mitigate risk

Risk Trend

Risk Action Owner(s) Enter a name or email address …

Risk Due Date

COO Comment (optional)

Risk Trend No

For more information please refer to the University Risk Framework
## Appendix 6

### Risk Profiles and Assurance Mapping

Risk profile charts provide an overview of the types and degree of risk and can be used at both operational and strategic level. Data can be aggregated by risk category or by project for example, and be provided to Committees or senior staff in order to promote discussions around risk.

<table>
<thead>
<tr>
<th>Almost Certain</th>
<th>Probable</th>
<th>Likely</th>
<th>Unlikely</th>
<th>Rare</th>
</tr>
</thead>
<tbody>
<tr>
<td>180 Albany Street</td>
<td>Basement Upgrade Marana Hall</td>
<td>Arts building</td>
<td>Fume Extractor - Botany</td>
<td>Bathroom Upgrade Exec. Residence</td>
</tr>
<tr>
<td>Dental School Building</td>
<td>Arana College Project</td>
<td>Hocken Library Extension</td>
<td>CFI Roof Replacement</td>
<td>Union Street Paving</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Negligible</th>
<th>Minor</th>
<th>Moderate</th>
<th>Serious</th>
<th>Very Serious</th>
</tr>
</thead>
</table>

Profile based on Risks in Subsidiary Risk Register

*Note: The above profile is based on fictitious data.*
Profile based on Categories of Risk

Note: The above profile is based on fictitious data.
Mitigation strategies and assurance providers can also be mapped to specific risks (i.e. the strategic risks of an organisation or to the projects “Top 10”) to identify gaps and/or to provide assurances that risks are being actively responded to.

<table>
<thead>
<tr>
<th>Top 10 Risks</th>
<th>Example Risk 1</th>
<th>Example Risk 2</th>
<th>Example Risk 3</th>
<th>Example Risk 4</th>
<th>Example Risk 5</th>
<th>Example Risk 6</th>
<th>Example Risk 7</th>
<th>Example Risk 8</th>
<th>Example Risk 9</th>
<th>Example Risk 10</th>
</tr>
</thead>
</table>

- **Strong Assurance** - lines of defence addressing risk, little or no further mitigation efforts required.
- **Partial Assurance** - some lines of defence addressing risk, further mitigation efforts may be required, monitor risk.
- **Assurance Gaps** - lines of defence not adequate, mitigation efforts required, risk may be external and not easily controlled, actively monitor and consider escalation.