Te Pātaka Kaupapa Here | UC Policy Library

Risk Management Framework

Nōnahea i Whakarerekē | Last Modified	December 2022
Rā Arotake | Review Date	October 2026
Mana Whakaae | Approval Authority	University Council
Āpiha Whakapā | Contact Officer	Director of Risk and Insurance – Planning, Finance and Digital Services

Kupu Whakataki | Introduction

The University is committed to managing its risks in a proactive, on-going and positive manner. This document outlines a structure for this process. This Framework is aligned with international best practice, key University planning documents, and our values of Whanaungatanga, Tiakitanga and Manaakitanga.

The Framework was first developed in February 2005, is approved by the University Council, reviewed informally every three years or as required, and formally every 5 years.

Contents

Kaupapa Here | Policy Statement

The University recognises that it must systematically manage and regularly update its risk profile at a strategic, operational, and programme or project level to explicitly address uncertainty and facilitate continuous improvement. The University has committed to this by developing a risk management 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 a number of international risk management standards, including *ISO 31000:2018 Risk Management – Guidelines (International Organisation for Standardisation (ISO) website)),* and *AS/NZ ISO 31000:2009 Risk Management Principles and Guidelines (Standards NZ website)*[1] (both referred to as "the standards") and key University strategic, operational and programme or 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 *Section 2* below.

The framework is managed within the risk management portfolio of Planning Finance and Digital Services, 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 Leadership Team (SLT). The Register is considered by the Senior Leadership Team, the Risk Advisory Committee, the Audit and Risk Committee, and the University Council. Content and recommendations are used to

[1] The ISO released revised standards in 2018 but this has not been formally adopted by Standards NZ. Therefore, both standards are referred to and may be purchased from the Standards New Zealand website.

inform the University's compliance obligations, internal audit programme, and subsequent iterations of the Strategic Risk Register.

As part of the risk management process, the University appreciates that one of its core risks is compliance with statutory obligations. It is thus committed to not only identifying the legislation with which it is obliged to comply, but also monitoring the levels of compliance in the institution and implementing change and/or mitigations where necessary. One way in which this is done is by adoption of the "Three Lines of Defence" model (see *Section 5: Monitoring and Review* and *Appendix A: Three Lines of Defence Model* for further details).

1. Risk Explained

1.1 What is a Risk?

A risk is the effect of uncertainty on objectives, i.e., 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 ('upside risk') or detrimental ('downside risk') 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.

1.2 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: strategic risks may also be 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 resources, the risks inherent in the organisational structure, and the way core operations are performed.

Project Risks are risks associated with programmes or 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 activities.

Programme or Project Sponsors are accountable for the achievement of deliverables and outcomes and benefits. However, specific risks associated with programme or project management are normally delegated to programme directors or project managers for attention and action. Included among the benefits of efficiently managing programme or 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.

1.3 Creating a Risk Statement

It is important that a risk is clearly and accurately articulated. The first consideration is to identify what is the actual risk. 'Cyber security breach' is not a risk, nor is 'loss of power'. Both may be root causes that give rise to a risk that then has consequences.

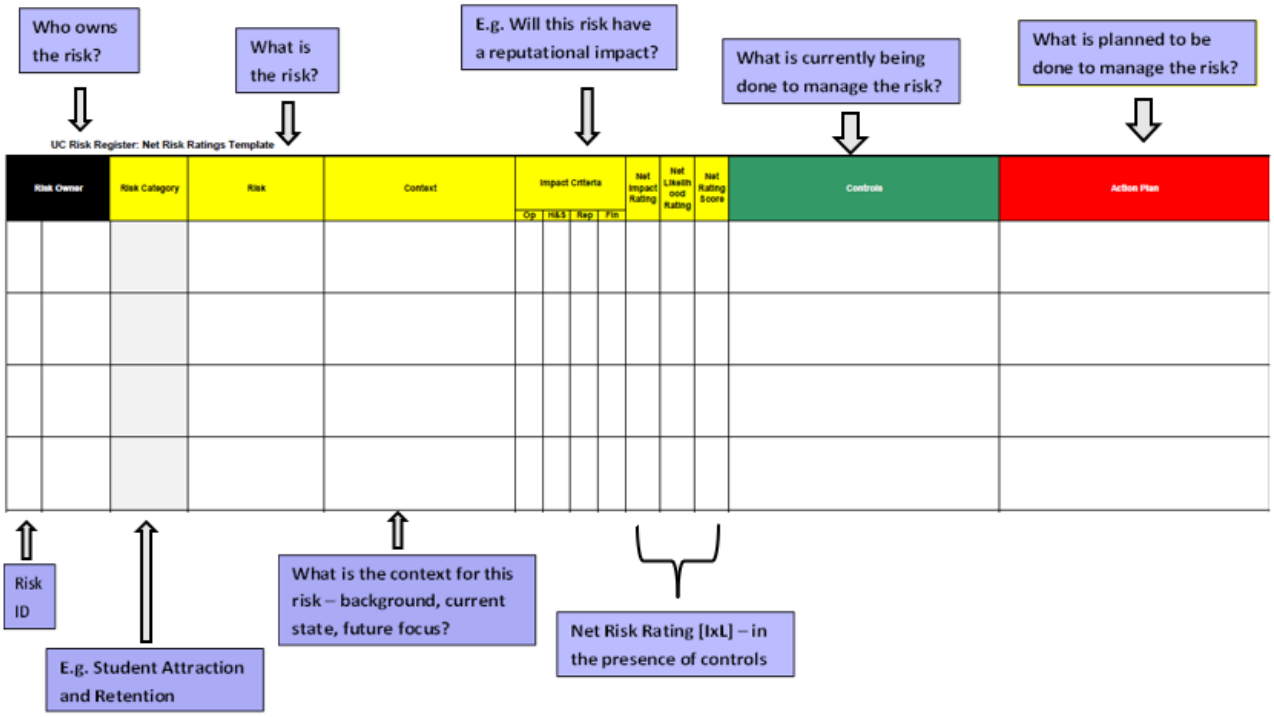
It is difficult to both measure and monitor risks that have not been described precisely.

To recap, what is a risk?

An uncertain event (**risk**), arising as a result of (**root cause**), impacts objectives (**consequences**)

Example: *"Critical data resources are not available (risk), as a result of a critical ICT systems failure (root cause), leading to service disruption (consequence)"*

1.4 The Risk Register Template



Note: The Risk Register may also include a trend column, showing whether the risk is increasing, decreasing, or static.

2. Governance and Management

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

Council	• Governance responsibility for risk management and legal compliance at the University of Canterbury. • Approval of Risk Management Framework
Audit & Risk Committee	• Governance oversight for risk management and legal compliance at the University of Canterbury.
Risk Advisory Committee	• Provision of risk advice and support to University management and governance committees about strategic, operational, and programme or project risk. • Management responsibility for implementation of the Risk Management Framework.
Vice-Chancellor	• Management responsibility of risk management and legal compliance. • Chair of Risk Advisory Committee.
Executive Director of Planning Finance & Digital Services	• Delegated responsibility for risk management University wide: risk policy, risk monitoring, and reporting to Audit and Risk Committee (see *The University UC Council Delegations Schedule (University Delegations of Authority webpage)*. • Management oversight of risk management on behalf of the Vice-Chancellor. • Assessment of the levels of acceptable risk and risk treatments and recommendations to the Vice-Chancellor accordingly. • Monitoring of Strategic Risk Register and regularly reporting to Audit and Risk Committee on management of risk issues. • Risk Management "champion" for the University.
Senior Leadership Team (SLT)	• Risk owners of strategic risks within the University. • Strategic and operational risk assessment, management, monitoring and reporting to the Executive Director of Planning Finance and Digital Services and/or the Risk and Insurance Manager for all risks relative to their areas of accountability.
Director of Risk and Insurance	• Management of the process of identifying and monitoring risk at the University. • Maintenance of Strategic Risk Register. • Monitoring of Strategic Risk Register and regularly reporting to Audit and Risk Committee on management of risk issues. • Responsibility for creating, implementing and disseminating Risk Management Framework. • Development of tools to assist the University community to implement best practice for risk and compliance matters. • Provision of expert advice, support, and training opportunities for all staff to promote a risk culture in the University. • Risk management 'promoter' for the University. • Assistance with the development of Operational and Project

	Risk Registers. • Publication/Dissemination of regular risk management information to keep staff informed of relevant risk issues.
Executive Deans and Service Unit Executive Directors	• Identification and analysis of strategic, operational and project risks within the Faculty/School/Unit; elevating risks where relevant to the Strategic Risk Register.
Director, Cybersecurity and Risk (Digital Services) Director of Health & Safety	• Consultation with Risk and Insurance Manager on relevant Digital Services and Health & Safety risks. • Escalation, where necessary, of Digital Services and Health & Safety risks to Strategic Risk Register.
Project Sponsors and Project Managers	• Assessment, management, monitoring and reporting of relative programme or project risks to relevant senior managers, Senior Leadership Team members and relevant committee/s or programme boards, with alignment to the Programme and Project Governance Framework.
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 Teams	• Advice to senior leadership 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 Leadership 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).*

3. Risk Management Programme

3.1 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, as articulated in the University Strategic Vision 2020 -

2030,

- 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 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 programme or 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 Strategic Vision 2020 – 2030, the University's Investment Plan (TEC) and other strategic plans (all available via the *University of Canterbury Governance website)*, and to support the national Tertiary Education Strategy.
- Risk being managed proactively in the University by knowledgeable staff using appropriate controls which are monitored regularly.

3.2 Approach

The University is committed to implementing a process by which strategic, operational and programme project risks (see Section 1.2 above) are identified, communicated, monitored and regularly reported, as appropriate, to Council (or other appropriate body). To facilitate this, a risk management framework has been developed for the University that proactively and systematically identifies, monitors, and manages risks. This framework aligns with the *ISO 31000:2018 Risk Management – Guidelines (International Organisation for Standardisation (ISO website),* and *AS/NZ ISO 31000:2009 Risk Management – Principles and Guidelines (Standards NZ website)* and the companion document *Australian/New Zealand Handbook Risk Management Guidelines [SA/SNZ HB 436:2013].* 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 and Insurance team. It is expected that these risks will both inform and be informed by the University Strategic Vision 2020 – 2030.

3.3 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.

3.4 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 Strategic Vision 2020 – 2030, it is necessary for both Governance and Management to know what degree of risk they are prepared to countenance in order to achieve the Strategic Vision 2020 – 2030. 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 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.

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 harm to students, staff, visitors or other stakeholders; significant reputational damage; financial damage; 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.

3.5 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, programme 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 **(Risk Retention)**.
2. Accept the risk but take some actions to lessen or minimise its likelihood or impact **(Risk Reduction)**.
3. Transfer the risk to another individual or organisation, by, for example, outsourcing the activity **(Risk Sharing)**.
4. Finance (insure against) the risk **(Insurance)**.
5. Eliminate the risk by ceasing to perform the activity causing it **(Risk Avoidance)**.

3.6 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 Faculty and Service Unit levels and input from Executive Deans, leadership 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 (or Inherent) 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 (or Residual) Risks – i.e., taking into account the aforementioned controls and documented accordingly.

By assessing risks as both Gross (Inherent) and Net (Residual), 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 Strategic Vision 2020 – 2030; the primary components of which are being engaged, empowered, and making a difference – tangata tū tangata ora. Within each of these components are strategic objectives that drive;

- successful civic engagement and social sustainability;
- successful internationalization (locally engaged, globally connected);
- successful learning and teaching (accessible, flexible, and future focused);
- high impact research (in a changing world);
- support wellbeing and success (nurturing staff, thriving students);
- environmentally sustainability; and
- economic sustainability and effectiveness.[2]

Potential Risk Categories

- Academic Quality
- Accreditation
- Attraction and Retention of Students
- Business Continuity
- Communication
- Compliance
- Emergency Management
- Ethics
- Health, Safety and Environmental
- Financial
- Internationalisation
- IT/Digital Delivery
- Programme Delivery
- Project/Asset Management
- Rankings

[2] UC Strategic Vision 2020 – 2030

- Recruitment and Retention of Staff
- Research (including both delivery of research and research outcomes)
- Research Integrity
- Strategic
- Service Delivery
- Staff and Student Wellbeing
- Stakeholder Relationships
- Sustainability

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:

Rating	%	Likelihood Criteria (within 12-24 months)
1	0 - 10	Highly unlikely to occur
2	10 - 25	Possibility of occurrence
3	25 - 75	Good possibility of occurrence
4	75 - 90	Likely to occur
5	90 - 100	Almost certain to occur

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.

Impact x Likelihood = 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.

Impact						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	**2**	**3**	**4**	**5**
		Likelihood				

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

Rating	
1, 2, 3	Minor
4, 5, 6	Moderate
8, 9, 10, 12	Significant
15, 16	Major
20, 25	Catastrophic

Key points to note when applying risk ratings

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

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

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

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

   At the action planning stage, management can then determine the risk treatment that needs to be applied to manage this risk down to a level that the organisation deems tolerable.

c) While this framework is based on a 5x5 matrix of assessment, it is appropriate from time to time to measure and document risk using the simpler 3x3 matrix of High, Medium,

and Low. Where this rating schema is applied, the alignment to the framework is as follows:

3x3 Matrix	Equivalent 5x5 Matrix
High	[15-25]: 5x5, 5x4, 4x5, 4x4, 5x3, 3x5
Medium	[8-12]: 4x3, 3x4, 5x2, 2x5, 3x3, 4x2, 2x4
Low	[1-6]: 3x2, 2x3, 5x1, 1x5, 2x2, 3x1, 1x3, 2x1, 1x2, 1x1

d) Risk assessments are not always neatly defined by multiplying the impact and likelihood ratings to determine a risk rating. Particularly in instances where life safety is paramount, the impact rating alone might drive risk-based decision making. By way of example, if there is an 'above normal' life safety risk, the likelihood of it being realized may not be a consideration. Instead, the risk of pursuing the activity may be unacceptable or intolerable. For the risk to be considered tolerable, the controls need to be such that the residual risk is deemed to make pursuit of the activity reasonable. Brown & Seville (2021) notes:

> *Between the two boundaries of acceptable and unacceptable risk, lies the concept of 'tolerable risk'. Tolerable risk is a level of risk that is higher than society finds 'acceptable' and should be mitigated/managed according to the ALARP principle – reducing the risk to be as low as reasonably practicable. Whether the residual level of risk can be 'tolerated' will depend on:*
>
> 1. *the importance of activities being undertaken,*
> 2. *whether they can be undertaken through other means, and*
> 3. *the cost of those mitigation measures*.[3]

See the Risk Appetite Statement and summary in *Appendix E*.

4. 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 area of risk, opportunities should also be provided for all staff to engage in regular training opportunities about relevant risk 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.

5. Monitoring and Review

Responsibility and accountability for monitoring and reviewing risks identified in strategic, operational and programme or project risk registers lie 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

[3] C Brown & E Seville: 2021. 'Future use of Kaikoura Field Station'. (August 2021), pg 7

Leadership Team. It is the expectation of Senior Leadership that any emerging/new strategic risks are brought to its attention by line management and risk owners within Faculties 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*.

6 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 and Insurance team regularly engages with risk owners across the organisation and consults with the Vice-Chancellor and the Risk Advisory Committee in developing reports, which are formally conveyed quarterly in full or in summary, to the Senior Leadership Team, the Risk Advisory Committee, the Audit & 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 and/or the global risk landscape.

Tautuhinga | Definitions

Action Plan – mitigations that are planned to further reduce a negative risk being realised or to enhance positive opportunities**.** Action Plans should be timebound and be assigned an action owner (who is not necessarily the risk owner). In the Risk Register, this can be recorded as per the following example [JL, 10/22] which means that JL is the action owner and is responsible for implementing the mitigation by October 2022].

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. These controls should be real and measurable and be updated each time the risk is reviewed.

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.

Issue – When a risk is realised, i.e., it is no longer an uncertain event because it has actually happened, it becomes an issue that needs to be managed under Business as Usual (BAU). Particularly at the programme or project level, it is relevant to maintain an Issues Register as well as a Risk Register.

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. Further elaboration on the definition of risk is provided in Section 1 below.

Risk Appetite – a high level statement that broadly considers the level of risk that management deems acceptable. The risk appetite sets the general level of risk that the organization accepts while pursuing its objectives before it decides to take any action to reduce that risk (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. Note that ‘Enterprise Risk Management’ or ‘ERM’ are terms that are also sometimes used to reflect risk management across an organisation.

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 Tolerance – the degree of variance from its risk appetite that an organization is willing to tolerate; (see *Appendix E*).

Risk Treatment – the process to modify risk (see *Section 3.5)* for an explanation of what a risk treatment, or management of a risk, might involve).

Note: Definitions are informed by the ISO 31000:2018 Risk Management – Guidelines, and AS/NZ ISO 31000:2009 Risk Management Principles and Guidelines (Standards NZ website) and the companion document Australian/New Zealand Handbook Risk Management Guidelines [SA/SNZ HB 436:2013] (Standards Australia website).

He kōrero anō | Related Documents and Information

Te Pātaka Kaupapa Here | UC Policy Library

- Conflict of Interest Policy Principles and Guidelines (PDF, 605KB)
- Fraud Response Policy and Procedures (PDF, 453KB)
- Privacy Policy (PDF, 744KB)
- Procurement Policy (PDF, 212KB)
- Protected Disclosures Act – Internal Procedures and Code of Conduct (PDF, 393KB)
- Sensitive Expenditure Policy (PDF 410KBy)
- Treasury Management Framework (PDF, 441KB)

Te Pae Tukutuku me te Ipurangiroto o UC | UC Website and Intranet

- UC Council Delegations Schedule 2006 – 2016 (PDF, 496KB) (University About UC Website
- Financial Delegations Register (University Financial Services intranet) (Staff Only)
- Plans, Policies and Regulations (University Governance website)
- UC Strategic Vision 2020 – 2030 (University About UC website)

Mōwaho | External

- Australian/New Zealand Handbook Risk Management Guidelines [SA/SNZ HB 436:2013] (Standards Australia website)
- ISO 31000:2018 Risk Management – Guidelines (International Organisation for Standardisation (ISO) website)

- Institute of Internal Auditors' Position Paper, "The Three Lines of Defense in Effective Risk Management and Control", January 2013
- Joint Australian/New Zealand International Standard® Risk Management – Principles and Guidelines, [AS/NZS ISO 31000:2009] (Standards New Zealand website)
- Three Lines of Defence Model (Office of the Controller and Auditor-General of New Zealand website)

Appendices

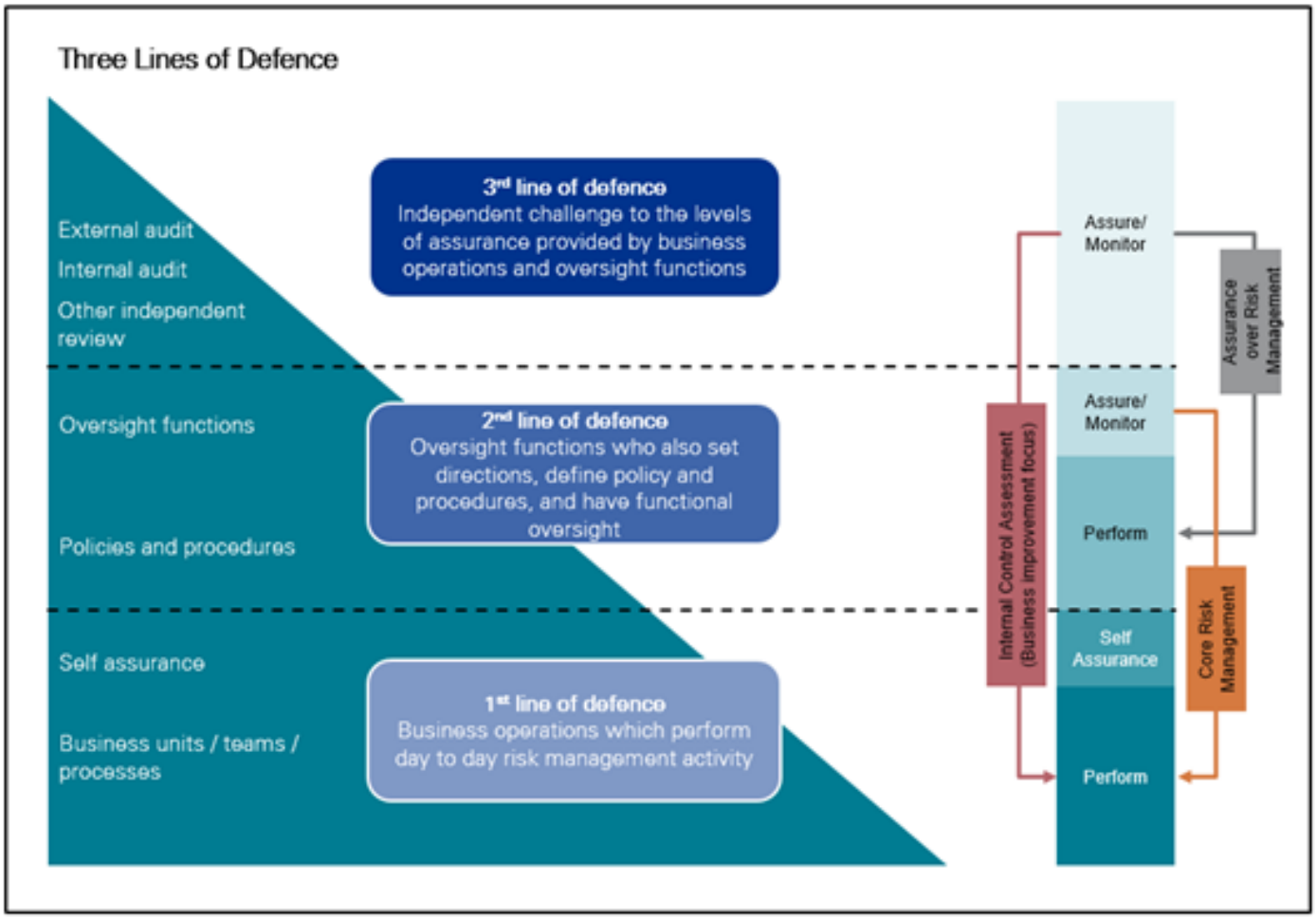
- Appendix A: Three Lines of Defence Model (Office of the Controller and Auditor-General of New Zealand website)
- Appendix B:The Governance, Risk and Compliance Model – reproduced with permission from PricewaterhouseCoopers
- Appendix C: Risk Culture Model – reproduced with permission from copyright owners, Dawson McDonald & Associates
- Appendix D: Relationships between the Risk Management Principles, Framework and Process [*Joint Australian/New Zealand International Standard® Risk Management – Principles and Guidelines,* AS/NZS ISO 31000:2009] – reproduced with permission from Standards New Zealand
- 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

Document History and Version Control Table			
Version	**Action**	**Approval Authority**	**Action Date**
1.00	Framework developed.	Chair, Council	Feb 2005
2.00	Full Review.	Deputy Vice-Chancellor	Feb 2008
3.00	Review to align with new standard: AS/NZS/ISO31000.	Chair, SMT	Jul 2010
3.01	Minor amendments to lines of responsibility (Section 1).	Chair, Audit & Risk Committee	Aug 2010
4.00	Full Review.	Audit & Risk Committee	Aug 2013
4.01	Minor amendment to Appendix B.	Audit & Risk Committee	Oct 2013
4.02	Change to C/O title.	Policy Unit	May 2014
4.03	C/O title updated throughout document.	Policy Unit	Mar 2015
4.04	Minor formatting change.	Policy Unit	Mar 2015
5.00	Full Review.	Audit & Risk Committee	Sep 2016
5.01	Changed title of Contact Officer from	Policy Unit	Jan 2017

	Senior Risk & Insurance Advisor to Risk Manager.		
5.02	CO referenced an updated ISO standard via footnote, addition of relevant legislation	Policy Unit	April 2018
5.03	Unscheduled review, inclusion of risk appetite statement, re-ordering of appendices, minor content changes	Policy Unit	Nov 2018
5.04	Unscheduled review by Contact Officer, minor changes to procedural information to reflect the approved Risk Advisory Committee functions	Policy Unit	Sep 2019
6.00	Schedule review by Contact Officer, minor change to content, change of document name	University Council	Oct 2021
6.01	Amended and Council approved risk appetite statement included	Policy Unit	March 2022
6.02	Role title updates, minor content changes	Policy Unit	Dec 2022

Appendix A: Three Lines of Defence Model

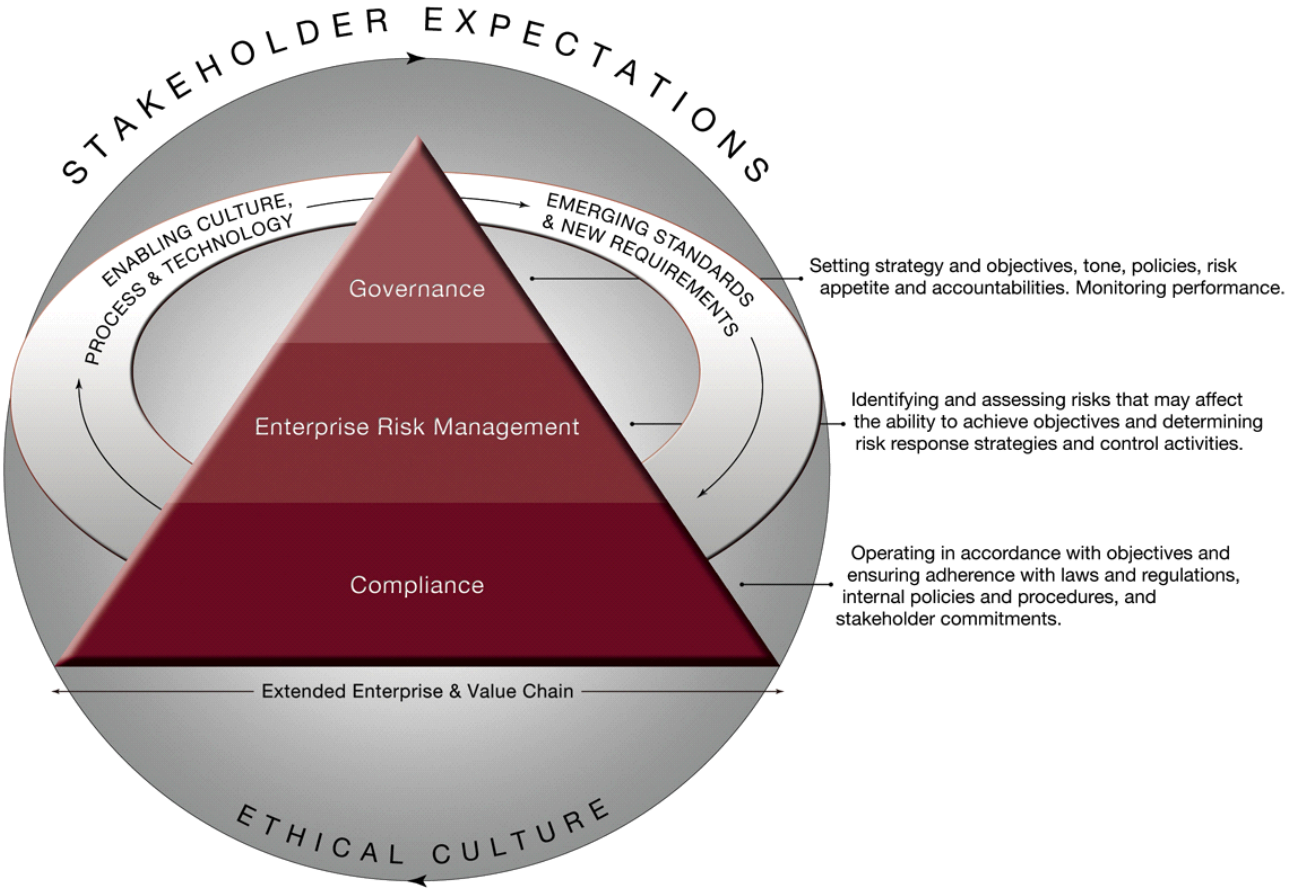
As noted by the Office of the Auditor-General of New Zealand, "the 'three lines of defence' model is useful as a clear and effective way to strengthen communications on risk management, assurance, and control by clarifying essential roles and duties for various parts of governance, management, and day-to-day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



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

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.



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)

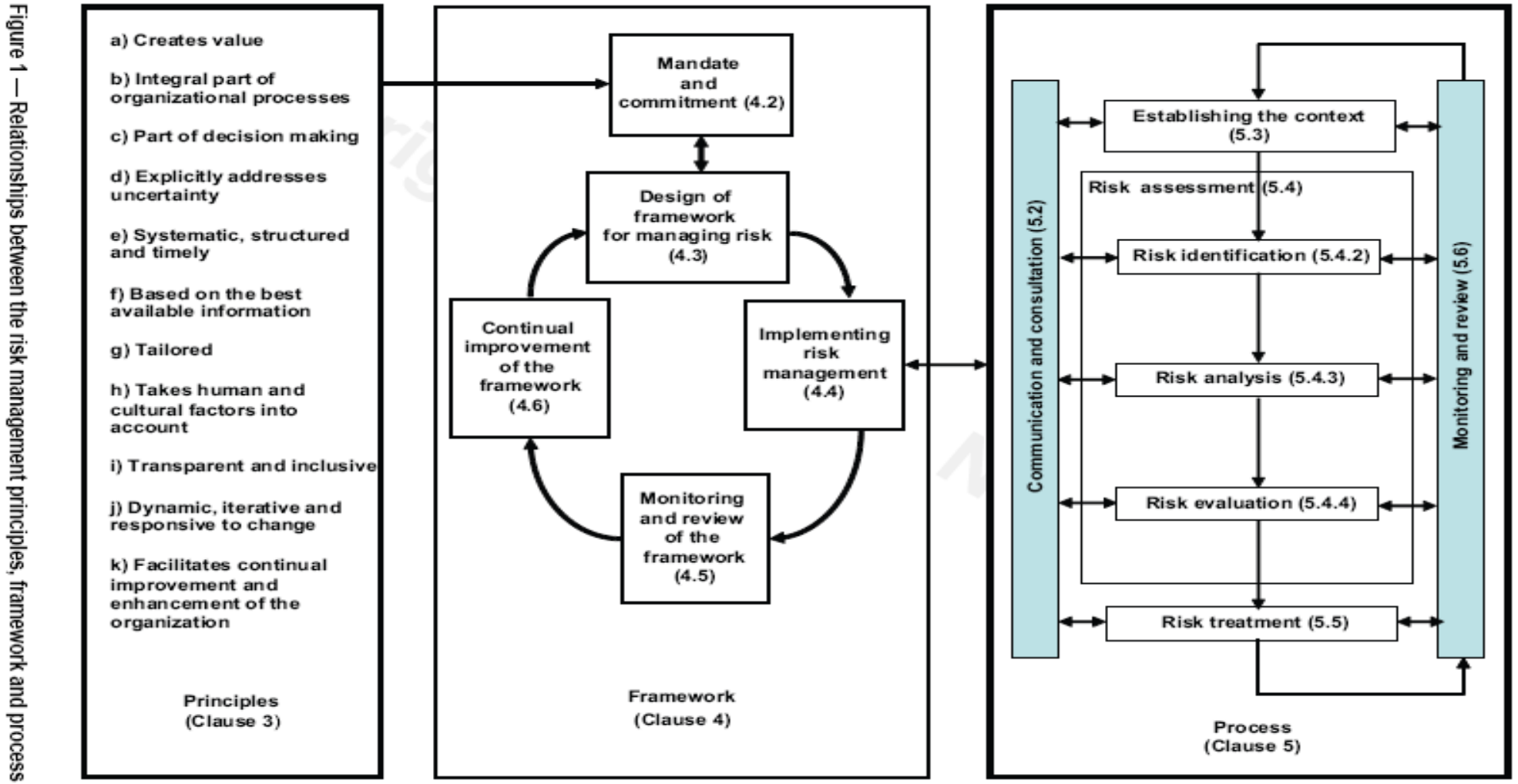
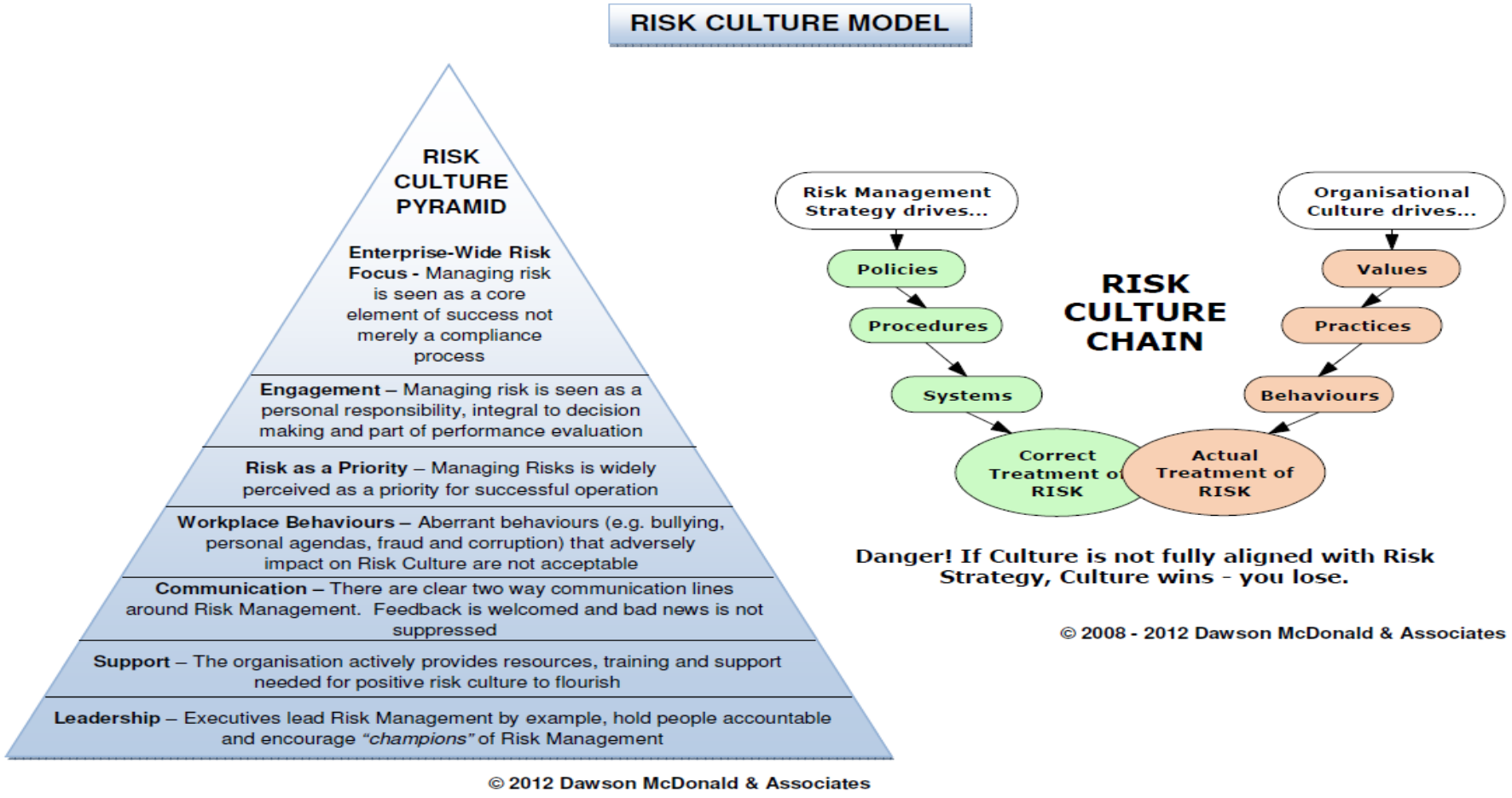


Figure 1 — Relationships between the risk management principles, framework and process

Appendix D: Risk Culture Model



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.

Risk Appetite Summary									
	Low Appetite			**Moderate Appetite**			**High Appetite**		
									
	Accept little or zero risk, taking a cautious approach towards taking risk			*A balanced and considered approach is adopted to taking risk*			*A more assertive or aggressive approach to taking risk is accepted to realise strategic objectives*		
Strategic Growth						<			>
Financial		<					>		
Compliance	<		>						
Privacy	<	>							
Health, Safety and Environmental	<	>							
Reputation			<			>			
Staff Wellbeing		<			>				
Student Wellbeing		<			>				
Cybersecurity	<			>					
Teaching Quality			<		>				
Teaching Accreditation			<		>				
Programme and Course Development						<		>	
Research Integrity	<		>						
Research Quality		<				>			
Research Initiatives						<			>

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 Strategic Vision 2020 – 2030. In order to achieve this, the University considers that it has a **high** appetite for risk in this area. One example in the programmes of work under way is the Kia Angitu – Student Success Programme, to make a significant impact on student success by providing targeted interventions and fostering a positive environment at the University.

Financial Risk

By 2020 UC had more than recovered from the revenue losses as a result of the earthquakes and was on a fast growth pathway for both Domestic and International EFTS and its cash reserves were high. The worldwide COVID-19 Pandemic hit NZ on 25 March 2020 with a Level 4 lockdown NZ wide and this hit the University hard especially with International EFTS which fell swiftly as the borders closed. This persisted into 2021 with further drops in International EFTS and this seems likely to continue into 2022. By this time the International cohort at UC will be very small. Fortunately, the closed border has also contributed to a large increase in the domestic student cohort and this increase, which was funded fully by Government, has largely offset the loss of revenue from International student fees. Currently UC is in a relatively strong financial position with a strong cashflow and cash position especially when compared with other Universities in NZ, many of which are borrowing. UC is therefore in a strong position to invest in growth activities in line with UC Strategy to advantage its position compared to its competitor Universities and take a higher level of risk than it has previously. The University also has overall responsibility for around $180M of trust funds for which it would have a low appetite for risk given the impact on future and past donors and the University's reputation.

While the risk appetite in this area spans the low, moderate and high risk categories, the University considers that it has a predominantly **low** to **moderate** appetite for financial risk.

Compliance Risk

The University recognises its compliance obligations, through legislation, including with the Education & Training Act, Health & Safety at Work Act, Official Information Act, Privacy Act, Public Finance Act, and the Education (Pastoral Care of Tertiary and International Learners) Code of Practice, as well as University 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.

Privacy Risk

The University recognises its privacy obligations under the Privacy Act 2020. The University commits to upholding the Privacy Act's thirteen information privacy principles. This includes: only collecting personal information for a lawful purpose connected to the University; collecting information directly from the individual; being open about why we're collecting the information; having safeguards about storage to prevent loss and misuse;

allowing access to a person's own personal information, including for correction; ensuring accuracy and appropriate retention; and only using private information for the purpose collected. The University has a low appetite for any breaches that cause adverse impact to individuals, including avoiding loss, damage, adversely affecting the rights and benefits, or causing significant humiliation or loss of dignity to an individual. The University considers that it has a **low** appetite for risk in this area.

Health, Safety and Environmental Risk

The University acknowledges its obligations as a Person in Control of a Business or Undertaking (PCBU) under the Health & Safety at Work Act 2015. Further, it anticipates that staff, students, contractors, and visitors should expect that this is a safe place to work and study. The appetite to accept risks to the health and safety of staff, students and others on our campuses is very low. It is not our intention to avoid inherently risky activities which are part of running a University; however, a strong culture of health and safety awareness and risk management is expected of all staff. This includes identifying and managing health and safety risks so far as reasonably practicable. We have a strong interest in protecting and preserving the environment, hence, have a low-risk appetite for activities which will significantly degrade the environment. The University thus considers that it has a **low** appetite for risk in this area.

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.

Staff and Student Wellbeing Risk

A number of stressors, including the Canterbury earthquakes, the terrorist mosque attacks in Christchurch, and the global pandemic have created an environment whereby the risk is increased of staff and students experiencing a range of wellbeing issues.

Staff Wellbeing

One of the four main objectives of the Health and Safety at Work Act is to protect people from the risk of injury or ill health by ensuring employees' health, safety and welfare at work. A person conducting a business or undertaking (PCBU) must ensure, as far as reasonably practicable, the health and safety of workers, and that other persons are not put at risk by its work.

Student Wellbeing

The introduction of the *Pastoral Care of Tertiary and International Learners Code of Practice* (with effect from January 2022) places obligations on UC to appropriately respond and resource that response. In addition, the UC equity review (August 2021) has illustrated that UC has systemic barriers that must be addressed.

The University, therefore, considers that is has a **low to moderate** appetite in this area.

Cybersecurity Risk

UC has a **low** appetite for the loss or breach of high-value information assets due to cyber-attacks and the unavailability of high-value information assets after an attack.

UC will take a balanced approach to cloud risk and has a **low** to **moderate** risk appetite for cloud adoption to allow the University to meet its strategic objectives.

The University considers its risk appetite in this area to be **low** 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; however, with the rapid move to online and in line with the UC Strategy to widen participation, traditional measures of teaching quality need review. 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 Engineering New Zealand (EngNZ) and the New Zealand Speech-Language Therapists' Association; however, the University recognises that it should be leading in terms of pedagogy, rather than following, and hence be willing to challenge thinking in the accreditation space. The University, therefore, considers that it has a **low to moderate** appetite for risk in this area.

Programme and Course Development

In its 2020-30 Strategic Vision, UC outlines a clear strategy that will require substantial change. UC seeks to provide accessible, flexible, and future-focused education. In working towards these goals, UC is exploring innovative teaching programmes, using flexible delivery options, and working in a built environment that is increasingly tailored for disruptive technologies and future-focussed needs. 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 Integrity

Research integrity is understood to encompass a) compliance obligations of Human and Animal Ethics under various regulatory bodies like the Ministry of Primary Industries, b) academic research codes of conduct, c) emerging consideration of appropriate international collaboration, and d) due regard of Protective Security Requirements. The University considers its risk appetite in this area to be **low** in nature.

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, bibliometrics of research, publications, peer-review and external bench-marking. The University considers its risk appetite in this area to be largely **low** to **moderate** in nature.

Research Initiatives

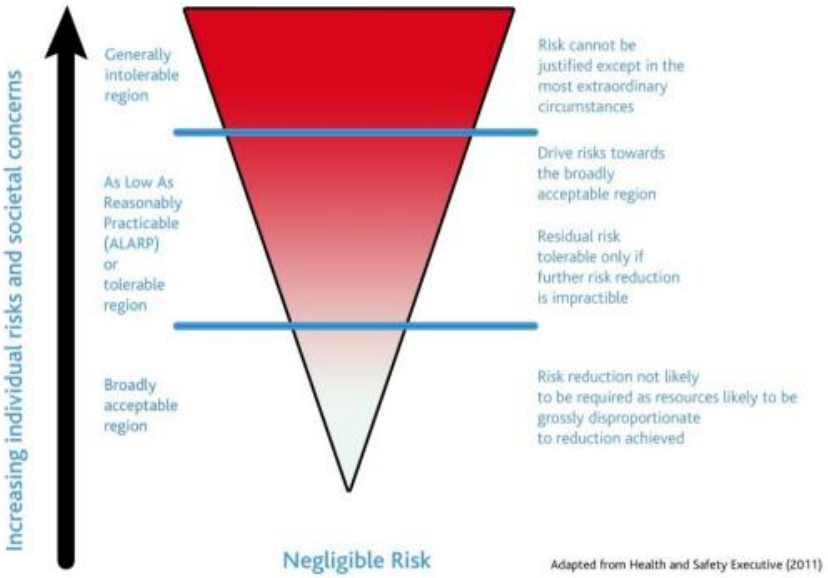
Research is by definition, a process of coherent inquiry, where the endpoint is unknown. Research is risky, where potentially the riskiest research might have the greatest impact in a specific field of knowledge and / or greatest societal impact. UC has a high appetite for initiating risky research, which leverage UC's particular research expertise and capacity, but also has a process to assess whether such initiatives and investments are "returning benefit" (including contributing to research revenue, postgraduate student growth, and innovative collaborative research opportunities), and if not, then to withdraw from such initiatives. The University considers that it has a **high** appetite for risk in this area.

Risk Tolerance and Treatment Levels

The Risk Appetite statement, while providing useful guidelines about the University's appetite for risk, does not address tolerance and treatment levels for each risk, particularly those that sit at the strategic level. The following table has been drafted to provide this guidance.

The University of Canterbury's Risk Appetite statement informs risk tolerances which, in practice, are on a continuum that runs from a conservative (low appetite) to an entrepreneurial/innovative (high appetite) view of risk. At the individual strategic risk level, however, the tolerances and treatments follow the guidelines below:	
20-25	Intolerable: urgent management attention and intervention required. - Consider options for reducing the impact or likelihood of the risk being realised: including ceasing associated activity, financing the risk, outsourcing the risk, and/or implementing mitigation strategies that are actioned within a 3-6 month timeframe.
15-16	Tolerable level of risk: significant management and monitoring required. - Consider options for reducing the impact or likelihood of the risk being realised: implement mitigation strategies that ensure the net risk rating is As Low as Reasonably Practicable (ALARP)**. Ensure that identified controls are tested regularly and are robust.
8-12	Tolerable level of risk: risk treatment strategies required, including testing of the robustness of controls and regular review of action plan items.
4-6	Acceptable tolerance levels: to be managed under normal control procedures.
1-3	Acceptable tolerance levels: to be managed under normal control procedures.

** ALARP Model



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

Rating		Impact Criteria			
		Operational	**Health and Safety**	**Reputational**	**Financial**
		Student number or teaching and/or research impact	**Degree of Harm**	**Level of Interest**	**$ Value**
1.	Minor	Minor reduction of students [8]. Undesired loss of staff member [1]. Minor impact on organisational strategic goals and operational activities.	Minor incident, no medical attention required. Event report submitted to Health and Safety.	Minimal public or local interest. Event that involves HOD/HOS management time.	Less than $100k in any 12-month period.
2.	Moderate	Moderate reduction of students [80]. Undesired loss of staff members [10]. Moderate impact on organisational strategic goals and operational activities.	Incident requiring moderate medical attention. Event report submitted to Health and Safety.	Moderate public or local interest. Event that involves College Manager/Direct Report management time.	$100k to $5m in any 12-month period.
3.	Significant	Undesirable reduction of staff and students in a course. Undesired loss of an academic course. Significant impact on organisational strategic goals and operational activities.	Incident requiring significant medical attention. Event report & investigation submitted to Health and Safety. Assault of a student or staff member.	Significant public or local interest. Event that involves PVC/AVC management time. Allegation of fraud/misconduct.	$5m to $10m in any 12-month period.
4.	Major	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.	Serious harm event or near miss. Event report submitted to Health and Safety. Event investigation submitted to Health & Safety. Serious harm event reported to Ministry of Business, Innovation & Employment or other relevant authority by Health & Safety Manager*. Student/Staff fatalities (off campus and non UC related activity).	Major public or media attention. Event that involves VC/ Audit & Risk Committee management time. Fraud by staff or contractor.	$10m to in any 12-month period.
5.	Catastrophic	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.	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 & Safety Manager+. Event report submitted to Health and Safety. Event investigation submitted to Health & Safety.	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.	Greater than $20m in any 12-month period.

Likelihood Criteria

Rating	%	Likelihood Criteria (within 12-24 months)	Guide for consideration of health, safety, and environmental risks
1	0 - 10	Highly unlikely to occur	(1 in 100-year event) No history of occurrence, the event is not expected to occur or only in conditions previously not seen
2	10 - 25	Possibility of occurrence	(1 in 50-year event) Little history of occurrence, the event may occur in typical circumstances
3	25 - 75	Good possibility of occurrence	(1 in 10-year event) History of frequent occurrence, the event may occur in typical circumstances
4	75 - 90	Likely to occur	(1 in 5-year event) History of frequent occurrence, the event will probably occur
5	90 - 100	Almost certain to occur	(annual event) History of regular occurrence, the event is expected to occur in most circumstances

Risk Rating = Impact * Likelihood

Impact					
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5
	1	2	3	4	5
			Likelihood		

Note: * Near misses are not generally reported to WorkSafe New Zealand)- refer Health and Safety at Work Act 2015 No 70 (as at 01 December 2020), Public Act – New Zealand Legislation for definition of notifiable illness, notifiable incident and notifiable event.
October 2021

Appendix H: Overall Risk Rating Matrix

Likelihood

Almost Certain *(5)*	**Moderate *(5)***	**Significant *(10)***	**Major *(15)***	**Catastrophic *(20)***	**Catastrophic *(25)***
Likely *(4)*	**Moderate *(4)***	**Significant *(8)***	**Significant *(12)***	**Major *(16)***	**Catastrophic *(20)***
Good Possibility *(3)*	**Minor *(3)***	**Moderate *(6)***	**Significant *(9)***	**Significant *(12)***	**Major *(15)***
Possible *(2)*	**Minor *(2)***	**Moderate *(4)***	**Moderate *(6)***	**Significant *(8)***	**Significant *(10)***
Highly Unlikely *(1)*	**Minor *(1)***	**Minor *(2)***	**Minor *(3)***	**Moderate *(4)***	**Moderate *(5)***
	Minor *(1)*	**Moderate *(2)***	**Significant *(3)***	**Major *(4)***	**Catastrophic *(5)***

Impact

(20-25) (15-16)	Catastrophic and Major	Risk Treatment Strategies to be implemented by Directors/Executives and, where relevant, action taken to be reported, either directly or via Senior Leadership Team Members, to the Risk and Insurance Manager for inclusion for discussion by the Risk Advisory Committee (RAC) and likely inclusion in the UC Strategic Risk Registrar.
(8-12)	Significant	Risk Treatment Strategies to be implemented by Directors/Executives.
(4-6) (1-3)	Moderate and Minor	Acceptable – to be managed under normal control procedures.