Compliance Management Framework

June 2024

University Operations

Risk, Assurance and Compliance

Campus and Collegiate Life Services | Campus Development | Chief Operating Officer
Health and Safety Compliance | Information Technology Services | Project Management
Property Services | Student Services | Sustainability

University of Otago | PO Box 56 | Dunedin 9054 | New Zealand

Enable | Engage | Experience

Contents

Document Control					
Version No.	**Date**	**Revision Details**	**Author**	**Endorsed**	**Approved**
1.0	July 2018	First draft	M.Cartwright	Audit&Risk Committee	Council
1.1	June 2024	Amended following release of ISO 37301:2021	M.Cartwright		Council

1. Purpose

The purpose of the Compliance Management Framework is to provide the basis for the development and maintenance of a coordinated set of activities to help ensure the University complies with obligations created by various instruments such as laws, regulations, industry codes, standards and University policies.

The framework also demonstrates the University's commitment to good corporate governance and ethical conduct. It is based on recommended practices described in the international standard ISO 37301:2021 "Compliance Management Systems" and provides:

- Guidance for developing, implementing, evaluating and maintaining an effective compliance management programme.
- Responsibilities and accountabilities for compliance management across the University.
- Procedures for the reporting and management of noncompliance.

2. Benefits

The Compliance Management Framework and associated activities:

- Reduce the risk of financial penalties or criminal prosecution.
- Reduce the risk of damage to individual/University reputation.
- Contributes to a robust and ethical culture of excellence in academic and corporate governance.
- Provide assurances to the Vice-Chancellor and Council that compliance risks are being managed.
- Encourages staff to respond appropriately to potential or actual noncompliance.
- Provides a uniform approach to support compliance with obligations that are relevant to the University's operations.

3. Compliance Governance

Compliance governance refers to the culture and arrangements developed by the University to manage its compliance obligations and its response to noncompliance risks. It includes leadership, accountabilities and oversight and is an essential part of the University's overall governance responsibilities.

The implementation of the Compliance Management Framework will promote principles of:

- Proportionality – the use of compliance activities that are targeted, cost-effective and reasonable.
- Transparency – actions and decisions made with impartiality and integrity.
- Consistency – through the development of explanatory materials and guidance for staff.
- Accountability – by clearly defining compliance management roles and responsibilities.

3.1 The Three Lines of Defence

The Three Lines of Defence Model[1] is designed to ensure the effective and transparent management of compliance obligations and risks 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 compliance management processes.

[1] The Institute of Internal Auditors. (2013). *The Three Lines of Defence in Effective Risk Management and Control.* Almonte Springs. IIA Global.

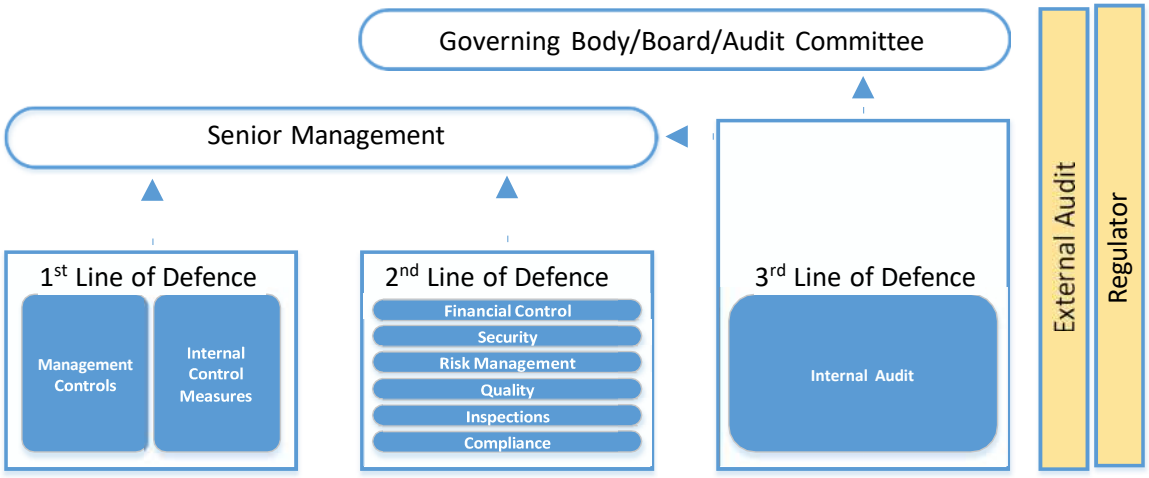

Figure 1: Three Lines of Defence Model

- First line of defence – University Operations, academic and operational management has ownership, responsibility and accountability for directly assessing, controlling and responding to compliance obligations.
- Second line of defence – consists of oversight and support functions such as risk management, compliance, quality, and finance.
- Third line of defence – Internal Audit, External Audit, regulators and other assurance providers who independently challenge both the first and second lines of defence.

4. The Compliance Management Process

The compliance management process is summarised in the following diagram and is based on elements contained in the international standard ISO 37301:2021 "Compliance Management Systems – Guidelines":

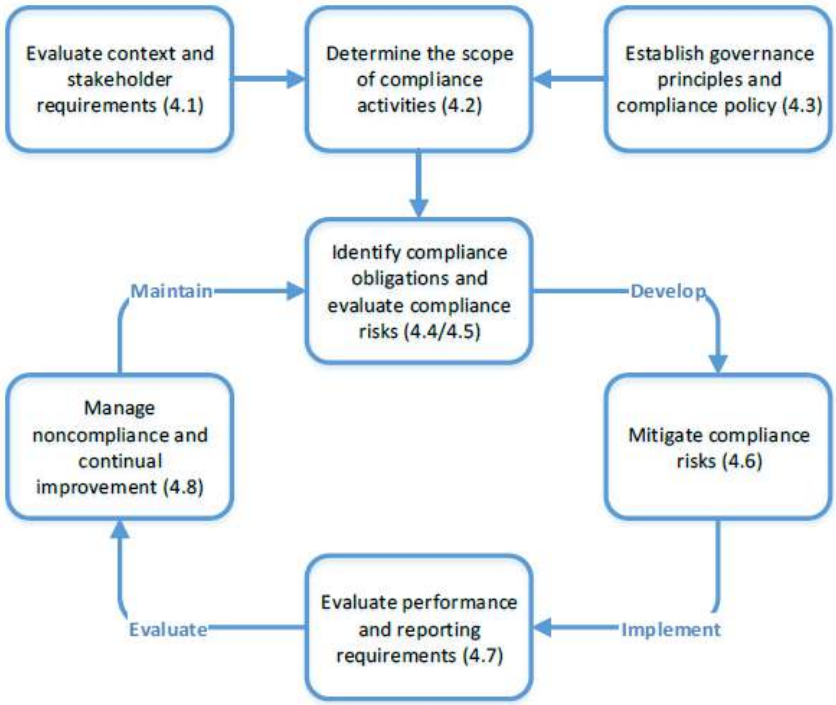

Figure 2: Compliance Management Process

4.1 Context

The context in which the compliance management process will be applied will involve an evaluation of the following:

Identification of External and Internal Issues:

- The legal, regulatory, social, cultural, financial, technological and economic environment in which the University operates.
- Key legislative and regulatory requirements.
- University structure, culture, roles and responsibilities.
- Internal policies, procedures, processes and resources.

Identification of Stakeholder Requirements:

- The stakeholders that are relevant to the compliance management system i.e. regulators, government agencies.
- The requirements of these stakeholders.

4.2 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 compliance management activities and provide reports on the status of compliance to the University's Audit & Risk Committee annually and on the request of the Committee.

4.3 Compliance Management Policy

The Compliance Management Policy is a high level document that outlines the purpose, objectives and governance arrangements for managing the compliance management programme. If provides guidance and helps to clarify expectations regarding the reporting of noncompliance and accountabilities relating to compliance management. A copy of the Compliance Management Policy is located in the Policy Library on the University's website.

4.4 Identification of Compliance Obligations

The University will systematically identify its compliance obligations and their implications for its activities and services. They will be recorded in a web-based Register of Compliance Obligations (Logic Manager). Processes will also be adopted to identify and implement changes in the management of compliance obligations when any new or changed laws, regulations and codes are introduced. This will involve the following activities but may also involve assistance from specialist external providers due to complex regulatory environment in which the University operates.

The sources for the identification of compliance obligations include:

- Engagement with management and other key staff in Divisions.
- Laws and regulations.
- Permits, licences or other forms of authorisation.
- Orders, rules or guidance issues by regulatory agencies.
- Judgements of courts or administrative tribunals.
- Treaties, conventions and protocols.
- Internal policies and procedures.
- Voluntary principals or codes of practice.
- Commentary sourced from the public domain.
- Membership of professional groups.
- Subscriptions to relevant information services.
- Attending industry forums and seminars.
- Monitoring regulators (websites, mailing lists, meetings, media).

The Register of Compliance Obligations

The Register of Compliance Obligations is located in the University's enterprise-wide risk management system (Logic Manager) which is accessible from the University's website. Instructions for accessing the Register can be obtained from the Office of Risk, Assurance and Compliance. The Register has been designed to capture compliance obligations, facilitate an enterprise-wide response to compliance obligations, and record remediation of actual or potential noncompliance.

The register will cross-reference, not duplicate obligations and remediation actions recorded in existing registers or systems at the University i.e. Health and Safety.

Compliance obligations will be grouped by type, for example:

- Agreements.
- Building.
- Contracts.
- Commercial Activities.
- Education.
- Environment.
- Equity.
- Food and Alcohol.
- Hazardous Substances.
- Industrial and Employment.
- Information Technology.
- Intellectual Property.
- International Students.
- Privacy and Records.
- Property Management.
- Research Ethics and Integrity.
- Security.
- Tax, Finance and Procurement.

To facilitate reporting and ongoing evaluations the obligations will also be mapped to the risk categories established in the University's Risk Management Framework (a copy of which can be accessed on the University's website):

- Environmental.
- External Relationships and Partnerships.
- Financial and Economic.
- Learning, Teaching and the Student Experience.
- Organisational Management.
- Property and Facilities.
- Research & Enterprise.
- Service Quality.
- Staffing and Human Resources.
- Workplace Health and Safety.

All staff, students and other stakeholders will be able to access detailed lists of the University's obligations, to whom responsibility has been assigned for ensuring compliance, and to whom any potential or actual compliance breaches may be reported. Access to some sections of the register will be controlled. Details regarding the progress of remedial or other actions taken to ensure compliance, for example, will be limited to Responsible Officers and their delegates.

Description	All Stakeholders	Responsible Officer
Obligations type	X	X
Obligation title	X	X
Risk category/s	X	X
Concise statements that capture the relevant internal/external obligation	X	X
Area of the University affected by the compliance obligation	X	X
Responsible Officer	X	X
Reports to whom noncompliance or inquiries may be directed	X	X
Inherent Risk Rating		X
Residual Risk Rating		X
Classification (Tier)		X
Strategic or operational objective potentially impacted if noncompliant		X
Potential consequences of noncompliance		X
Summary of processes/procedures currently in place to ensure compliance		X
Last review date		X
Next scheduled review date		X

4.5 Compliance Risk Assessments

When the identification of key obligations is complete, a compliance risk assessment will be undertaken and used as the basis for the implementation of the compliance management programme. Compliance obligations will be mapped to the University's activities and services to identify areas of potential noncompliance. They will then be risk rated and the outcomes used to prioritise the need for internal controls, reviews, training, monitoring and corrective action.

Risk assessment techniques will be a combination of desktop assessments, interviews, workshops and/or professional judgement and they will be aligned with the procedures and classifications detailed in the University's Risk Management Framework, a copy of which can be accessed on the University's website.
Care will also be exercised when evaluating the requirements of complex laws or regulations. If those undertaking the risk assessment are not appropriately qualified, there is a risk of differing interpretations of ambiguous, untested, or understated parts of laws or regulations. On that basis, the risk assessments will be undertaken in close consultation with management and if necessary external/specialist advice will be sought.

The categorisation of an obligation as High Risk will not be an indicator of noncompliance or that compliance risks are not being managed. This risk based approach helps to ensure the University focuses primary attention and resources on higher risks in priority order only.

In addition, the categorisation of an obligation as low risk should not be interpreted as meaning that for these situations, noncompliance is accepted by the University.

In brief:

1. The Register of Compliance Obligations is populated with applicable laws and regulations. When the compliance programme is sufficiently mature it will also include Council approved policies and procedures.
2. Following consultation with Divisions, and subsequent process, data and other reviews, obligations will classified according to *residual risk* (i.e. the risk to the University after the operation of mitigating controls have been assessed), classifications being Very High (Tier 1), High (Tier 2), Medium (Tier 3), Low (Tier 4) – refer Risk Rating/Classification table in Appendix 1.
3. During consultations with Divisions additional obligations will be identified, risk rated and recorded in the Register of Compliance Obligations i.e. permits, licences, protocols, codes.
4. Responsible Officers will then be assigned to all Tier 1 and Tier 2 obligations.

4.6 Compliance Risk Mitigation

Management will be responsible for implementing controls to manage compliance obligations and associated risks. For each Tier 1 and Tier 2 obligation the University's risk management application (Logic Manager) will be populated with the following:

1. Compliance Obligations – a brief description of compliance requirements and consequences of a breach together with the inherent and residual risk ratings.
2. Assurance – a description of controls in place or required together with an assessment of their effectiveness in mitigating the risk of noncompliance.
3. Reporting Requirements – if applicable, type and frequency of reports required.

The maintenance of this information will assist with the monitoring of risk mitigation activities to ensure that they are effective and to identify any new or changed compliance risks.

It is anticipated that for a significant majority of obligations, existing strategies and controls to ensure compliance will already be adequate i.e. additional work/activities to ensure compliance will be minimised and will only need to be undertaken where compliance gaps, or significant weaknesses in controls, are identified.

4.7 Performance Evaluation and Compliance Reporting

4.7.1 Performance Indicators

Indicators will be established to help measure the effectiveness of the compliance programme. The measures may include for example:

- Training – percentage of staff receiving compliance training.
- Incidents – count of noncompliance issues by type, area and frequency.
- Consequences of noncompliance – fines, penalties, remediation costs.
- Noncompliance trends based on historical data – reduction in number of minor/major breaches over previous assessment period.
- Progress with plans – instances where internal compliance inspections have not been performed as scheduled.

Performance indicators will form part of reports submitted to the Audit & Risk Committee.

4.7.2 Reporting

Cyclical reporting arrangements for compliance activities will include:

Audit & Risk Committee

Quarterly reports on the performance of the compliance programme will be submitted to the Audit and Risk Committee by the Office of Risk, Assurance and Compliance. These reports will include a high-level summary of activities by all functions undertaking significant compliance related activities at the University i.e. building compliance, health and safety. These arrangements will not replace the existing reporting processes that these functions have in place and they will not create an additional reporting burden for these functions (i.e. existing reports/processes will be utilised).

Separate reports will also be submitted to the Audit and Risk Committee for major noncompliance incidents or emerging compliance issues.

Annual Certifications

At the end of each calendar year Responsible Officers will be required to provide an assurance that to the best of their knowledge, the University has complied with the obligations relevant to their area of responsibility. This process will be facilitated by the Office of Risk, Assurance and Compliance who will in turn prepare a consolidated report to the Chief Operating Officer, Vice-Chancellor and the Audit & Risk Committee on the overall outcomes of the certification process.

Regulatory Agencies

Internal and external regulatory reporting arrangements for compliance activities undertaken by the functions referred to in Section 5.2 of this framework remain unchanged. The reporting of significant compliance issues and risks (i.e. Very High, High) identified by these functions however must be undertaken in accordance with the procedures outlined in Section 4.8.1 of this framework if applicable.

4.8 Managing Noncompliance and Continual Improvement

4.8.1 Compliance Breach Escalation

All staff are required to report actual or potential noncompliance whether it involves their actions or the actions of someone else.

The following incidents for example, would require a report:

- Action being taken against the University by any government agency, statutory body, individual or company.
- Serious breaches of University policies or procedures.
- Cases of fraud or corrupt conduct.
- A breach that may create health and safety risks.
- A breach that may create media interest/reputational damage.
- Serious "near-misses".
- Regulatory sanctions (all events to be reported regardless of amount).

Reports should be prompt and in the first instance made to management or the most appropriate department listed under Section 5 of this framework, depending on the nature and significance of the breach.

The decision to escalate a report will invariably be based on professional judgement. If there is any uncertainty staff/management are encouraged to refer the matter to their senior manager, the Office of Risk, Assurance and Compliance or the Chief Operating Officer for advice.

A report should include the name of the legislation/policy breached, dates, people and areas involved (both internal and external), notifications made to regulatory authorities and steps taken to resolve the matter.

4.8.2 Confidential Reports

Staff are encouraged to raise any noncompliance concerns with their managers in the first instance. If staff have concerns regarding confidentiality and possible reprisals however, they may contact the University Disclosure Officer (refer the University's Protected Disclosures Policy) the Office of the Ombudsman, or the University's external auditor, Audit New Zealand, who will maintain confidentiality regarding the matter.

4.8.3 Closing of Compliance Management Plans

Management may close a noncompliance matter when the actions detailed in the Register of Compliance Obligations have been completed. The Audit & Risk Committee will be formally notified when remediation efforts involving significant compliance breaches have been completed. This notification will form part of regular reports to the Committee.

4.8.4 Continuous Improvement

The operation of the compliance management programme will be independently reviewed on at least a three yearly basis to ensure it is conforming to this framework and the requirements detailed in the Compliance Management Policy. This review may be undertaken by internal audit, an external specialist or by way of peer review.

4.9 Compliance Management Process Summary

Process Step	Undertaken By	Example Tools & Resources	Ref.
1. Consider context and stakeholder requirements	• Office of Risk, Assurance and Compliance.	• Annual reports. • Policy Library.	4.1
2. Establish scope of the compliance framework and programme	• Office of Risk, Assurance and Compliance	• Organisational charts. • Strategic and operational plans.	4.2
3. Establish a Compliance Management Policy	• Office of Risk, Assurance and Compliance	• Position Descriptions • Policy templates	4.3
4. Identify and record compliance obligations	• Office of Risk, Assurance and Compliance • Divisions	• NZ Legal Inform.Institute • Policy Library • Professional groups	4.4
5. Assess compliance risks and allocate obligations to Tiers	• Office of Risk, Assurance and Compliance • Divisions	• Risk Management Framework. • Interviews, workshops.	4.5
6. Record and implement/monitor remediation activities in the Register of Compliance Obligations (Logic Manager)	• Responsible Officers	• Staff consultation • Risk Mgmt Framework • Performance Indicators • Performance reports • Inspections	4.6
7. At year-end, complete an annual certification that provides assurances that compliance obligations have been met.	• Responsible Officers	• Self-assessments • Staff consultation • Audits, reviews	4.7

5. Related Compliance Activities and Programmes

5.1 Distribution of Compliance functions

Compliance tasks and activities can be managed using a centralised, decentralised, or hybrid model. Given the breadth and complexity of the University's operations, compliance activities outlined in this framework will be distributed across the University using a hybrid approach where some activities are managed centrally and other activities are managed by Divisions.

Functions managed centrally include:

- Quarterly reporting on the status of University-wide compliance activities to the Audit & Risk Committee.
- Oversight of the Annual Certification of Compliance process and associated reports to the Vice-Chancellor/Audit & Risk Committee.
- Ongoing co-ordination of activities associated with the implementation of the Compliance Management Framework.
- Coordination of compliance risk assessments.

Functions managed by Divisions include:

- Maintenance of entries in the Register of Compliance Obligations.
- Annual Certification of Compliance.
- Ensuring that noncompliance and noncompliant behaviours are dealt with appropriately.
- Maintenance of ongoing relationships with regulators.

Shared functions:

- Maintenance and update of the Register of Compliance Obligations.
- Provision of training and guidance to staff regarding compliance obligations.
- Identification of new or emerging compliance obligations.
- Encouraging employees to raise compliance concerns.

5.2 Related Compliance Activities

The hybrid approach also recognises that key compliance activities and programmes to promote compliance are already being made by Departments/Divisions as detailed below. On that basis no changes to the manner in which these functions operate are proposed i.e. the implementation of the Compliance Management Framework will be undertaken in close consultation with these functions to ensure information is shared and to minimise duplication of effort.

Corporate Records Services

This department manages the implementation of the University's records management framework. The framework helps to ensures that full and accurate records of the University's activities are created, captured, maintained, made accessible, stored and legally disposed of in accordance with legislative requirements.

Financial Services Division

The Financial Services Division contributes to the management of compliance obligations through its maintenance of financial planning, performance and reporting systems. Significant strategic and operational obligations relating to budgets, expenditure, financial statements, delegations and procurement are managed by its financial and management accounting functions.

Its functions also include accounts payable, revenue management and supply chain. A wide range of internal controls are embedded into these activities to ensure expenditure, income and procurement transactions are undertaken in compliance with University policies and procedures.

Human Resources

The Human Resources Division works to create an environment that attracts, retains and develops the staff that the University needs to achieve its goals. It also ensures that staff comply with a wide range of employee conditions and benefits, as expressed in various employment agreements.

Information Technology Services

Information Technology Services is responsible for the provision, maintenance and support of information technologies within the University of Otago community. It undertakes a wide range of activities to ensure our systems meet best practice industry standards, particularly relating to the protection of the University's systems and data from external threats.

Internal and External Audit

The Internal Audit function undertakes ongoing assessments to obtain assurances that departments are operating in compliance with laws, regulations and the policies approved by the University Council. Compliance assessments are also routinely completed by the University's external auditors when undertaking financial statement audits.

Office of the Registrar

Policies govern University practice and support the achievement of the University's mission and objectives. Policies also support the achievement of quality outcomes and reduce institutional risk. Policy and Compliance oversee policies and procedures at the University to help ensure that they are consistent, practical, easy to implement and are appropriately approved.

Property Services Division

Staff in Building Compliance, Property Services Division undertake a cyclical range of checks to ensure buildings comply with building legislation and are safe to use. These checks range from fire extinguisher maintenance through to the risk of exposure to asbestos dust. They also ensure that Building Warrants of Fitness are in place.

Health, Safety and Wellbeing

The University of Otago's health and safety management structure supports and facilitates compliance with relevant Workplace Health and Safety legislation, codes of practice, guidelines and standards.

The University also maintains an online Health and Safety management system (Vault) that allows staff, students, contractors and visitors to the University campuses to report any health and safety related events or concerns.

6. Training and Support

The University will provide training to staff to ensure they are aware of and understand their compliance obligations and the need to promptly report actual or potential noncompliance.

Training will be:

- Tailored to the obligations and compliance risks related to the job role of the employee.
- Undertaken at employee induction and be ongoing.
- Aligned to professional development programmes administered by Human Resources.
- Recorded and evidence of training retained.
- Considered whenever there are changes in job roles, laws, or policies for example, or if significant issues arise following audits, reviews, complaints, feedback and instances of identified noncompliance.

Guidelines for specific compliance obligations will be developed and provided to staff to support this training. Additional ad-hoc training may also be provided when legislation or regulations are introduced or significantly amended.

7. Roles and Responsibilities

The development, implementation and maintenance of the Compliance Management Framework and the coordinating role performed by the Office of Risk, Assurance and Compliance should not be seen as absolving management of their compliance responsibilities.

In addition, outsourcing of operations or activities does not relieve management of its compliance obligations. The standard that would be required for any outsourcing contractor should be the same as that for the University itself. Management are expected to take all reasonable steps to ensure that our standards and commitment to compliance will not be lowered by any outsourcing agreement.

The roles and responsibilities of the Council, its Committees and staff are detailed in the Compliance Management Policy that can be accessed on the University website.

Additional roles include:

Responsible Officers

A Responsible Officer will be appointed for each compliance obligation that is risk rated as Very High or High:

The role of the Responsible Officer will include:

- Responsibility for ensuring the University complies with the designated compliance obligation.
- Providing guidance and support to staff regarding the obligation.
- Liaising with external parties including regulatory authorities and other interested parties as required.
- Reporting noncompliance with the obligation in accordance with the reporting and escalation procedures in Section 4.8.1.
- Develop and implement remediation activities recorded in the Registrar of Compliance Obligations for the legislation for which they are responsible.
- Provision of an Annual Certification of Compliance to the Vice-Chancellor.
- Determining training needs.

Internal Audit

The internal audit function will:

- Undertake regular independent reviews of the adequacy and effectiveness of the Compliance Management Framework and related compliance programme.
- Report outcomes to the Audit & Risk Committee.

8. Compliance Calendar

In order to ensure the smooth execution of the compliance programme, timebound activities to which the Divisions and the Office of Risk, Assurance and Compliance will need to adhere to, are summarised in a Compliance Calendar.

The activities recorded in the calendar will include:

- Formal reviews of the Register of Compliance Obligations to ensure it remains current.
- Regular oversight of remediation activities that address major compliance risks or instances of noncompliance.
- Annual Certification of Compliance process.
- Meetings/contact with key regulators.
- Formal reviews of past and current noncompliance to identify systemic issues/lessons learned.
- Annual reviews of the risk classification of Tier 1 and Tier 2 compliance obligations.
- Bi-annual reviews of the risk classification of Tier 3 and Tier 4 compliance obligations.
- Independent reviews of the operation of the Compliance Management Framework, at least every 3 years.

9. Contact Information

For further information regarding the Compliance Management Framework contact the Office of Audit & Risk Assessment or email risk.management@otago.ac.nz

Glossary of Terms

Code *– statement of practice developed internally or by an international, national or industry body or other organisation.*

Compliance *– meeting all the organisation's compliance obligations. Compliance is achieved by embedding it into the culture of an organisation and in the behavior and attitude of the person working for it.*

Compliance Management Framework *– a set of components that provide the foundations and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving compliance throughout the organisation.*

Compliance obligations – *requirements that an organisation mandatorily has to comply with as well as those that an organisation voluntarily chooses to comply with.*

Continual Improvement *– recurring activity to enhance performance.*

Monitoring *– determining the status of a system, a process or an activity.*

Noncompliance *– non-fulfillment of a compliance obligation, either deliberately or inadvertently. It involves circumstances where a compliance obligation has not been met or has only partially been met.*

Register of Compliance Obligations *– records all of the Universities obligations together with actions taken to remediate actual or potential noncompliance. The register will cross-reference, not duplicate, obligations and remediation actions recorded in existing registers or systems at the University i.e. Health and Safety*

Requirement *– need or expectation that is stated, generally implied or obligatory.*

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

Standards *– documented codes, good practices, charters, technical and industry standards deemed by an organisation to be relevant.*

Appendix 1

Overall Risk (L X I)	Likelihood (L)	Impact (I)	Risk Rating/Classification – Compliance Obligations	Required Action
Very High **≥ 15**	(5) Almost Certain • *Will undoubtedly happen* • *Greater than 80% chance*	(5) Very Serious	• Potential financial impact of $10,000,000 (Corp.)/$1,000,000 (Div.) or more in any 12 mth period • Detrimental impact on operations or major projects • Sustained loss in reputation • Sustained impact on services delivery or quality • Loss of public confidence in the University • Contractual, legislative, or regulatory non-compliance with certain litigation • Life threatening	• Immediate notification to Audit & Risk Committee • Requires immediate VC/DVC/PVC/ Senior Management attention • Requires a detailed Compliance Management Plan within 30 days
High **10 – 14**	(4) Probable • *Will probably happen* • *50 - 80% chance*	(4) Serious	• Potential financial impact of $5,000,000 (Corp.)/$500,000 (Div.) or more in any 12 month period • Major impact on operations or major projects • Serious loss in reputation • Serious impact on services or quality • Probable loss of public confidence in the University • Contractual, legislative, or regulatory non-compliance with probable litigation • Extensive injuries	• Requires prompt senior management action/ attention • Requires a detailed Compliance Management Plan within 60 days • Reported to Audit & Risk Committee
Medium **5 – 9**	(3) Likely • *Might happen* • *20 - 50% chance*	(3) Moderate	• Potential financial impact of $2,000,000 (Corp.)/$200,000 (Div.) or more in any 12 month period • Moderate impact on operations or major projects • Short-term loss in reputation • Moderate decline in services or quality • Possible loss of public confidence in the University • Contractual, legislative, or regulatory non-compliance with potential for litigation • Minor injuries	• Requires ongoing management of control effectiveness • Manage by specific monitoring or response procedures • May require a Compliance Management Plan
Low **3 - 4**	(2) Unlikely • *Not expected to happen* • *5 - 20% chance*	(2) Minor	• Potential financial impact of $1,000,000 (Corp.)/$100,000 (Div.) or more in any 12 month period • Minor impact on operations or major projects • No loss in reputation • Minor impact on services or quality • No loss of public confidence in the University • Contractual, legislative, or regulatory non-compliance but litigation unlikely • Potential for injury	• Manage by routine procedures • Monitor control effectiveness by local management • May require a Compliance Management Plan
1 - 2	(1) Rare • *Less than 5% chance.*	(1) Negligible	• Potential financial impact of $1,000,000 (Corp.)/$100,000 (Div.) or less in any 12 month period	• Impact to be absorbed by daily business running costs or managed through routine procedures