University of New England
Compliance Management Framework and Procedures

Document data:

Document type:	Framework and Procedures
Administering entity:	Audit and Risk Directorate
Records management system number:	D12/50959
Date approved:	4th October 2012
Approved by:	Vice-Chancellor
Indicative time for review:	Maximum 2 years from approval date
Responsibility for review:	Audit and Risk Directorate
Related policies or other documents:	Compliance Policy Risk Management Policy and Guidelines Code of Conduct Records Management Policy AS3806- 2006 Compliance programs
Staff contact for advice:	Legal Counsel and Executive Director of Governance Director Audit and Risk
Revision history:	

Table of Contents

Acknowledgements

We wish to thank and recognise the assistance of the Compliance Manager at UNSW and aknowledge that our template of the Compliance Obligations Register is based on the UNSW template. In addition we thank and acknowledge the Victorian Managed Insurance Authority as the primary source for the basis of our Framework and Procedures.

Section 1 : Compliance Management Framework

1. Purpose

The purpose of the Compliance Management Framework (the Framework) is to implement the University of New England's Compliance Policy – one component of an integrated Governance Risk Compliance (GRC) approach to effective corporate governance, enterprise risk management and corporate compliance with applicable laws and legislation.

Along with the Australian Standard *AS3806-2006 Compliance Programs,* the Audit Office of NSW has identified Compliance Management as a key component of corporate governance. This Framework establishes an appropriate strategic framework that defines the responsibilities of both management and employees and facilitates the implementation of robust practices for the effective management of compliance obligations.

Establishment of an effective compliance management framework will reduce and/or mitigate the following risks:

- Damage to UNE's reputation – especially through external agency investigations.
- Inadequate internal control systems that may lead to fraud, corruption and/or inefficiencies.
- Financial Loss.
- Staff health and safety issues not being met.

2. Scope

The Policy and this Framework apply to all employees and students of UNE and its controlled entities. Employees are those who are permanent, temporary or casual and include contractors and consultants.

Exclusions

Compliance framework and procedures falling within the portfolio of the Academic Board are outside the scope of this framework, except for, the provisions contained within section 8.1, Annual Reporting, of the Compliance Management Framework.

3. Compliance Management Introduction

The Compliance Management Framework is one component of an integrated GRC approach, and specifically consists of the policies, processes, tools and structures that help identify and manage the risks around meeting our objectives. It therefore has important links to the Risk Management Policy, and includes elements of both the risk management processes and internal control.

The Framework and Procedures provides the following information:

- An alphabetical listing of regulatory and business requirements. (Compliance Requirements Register).
- The obligations that each piece of legislation imposes (Compliance Obligations Register).
- Links to the policies and procedures developed by the University to address the requirements of each piece of legislation.
- Key contacts responsible for coordinating compliance with each Act.
- Training available to assist employees in meeting their obligations.

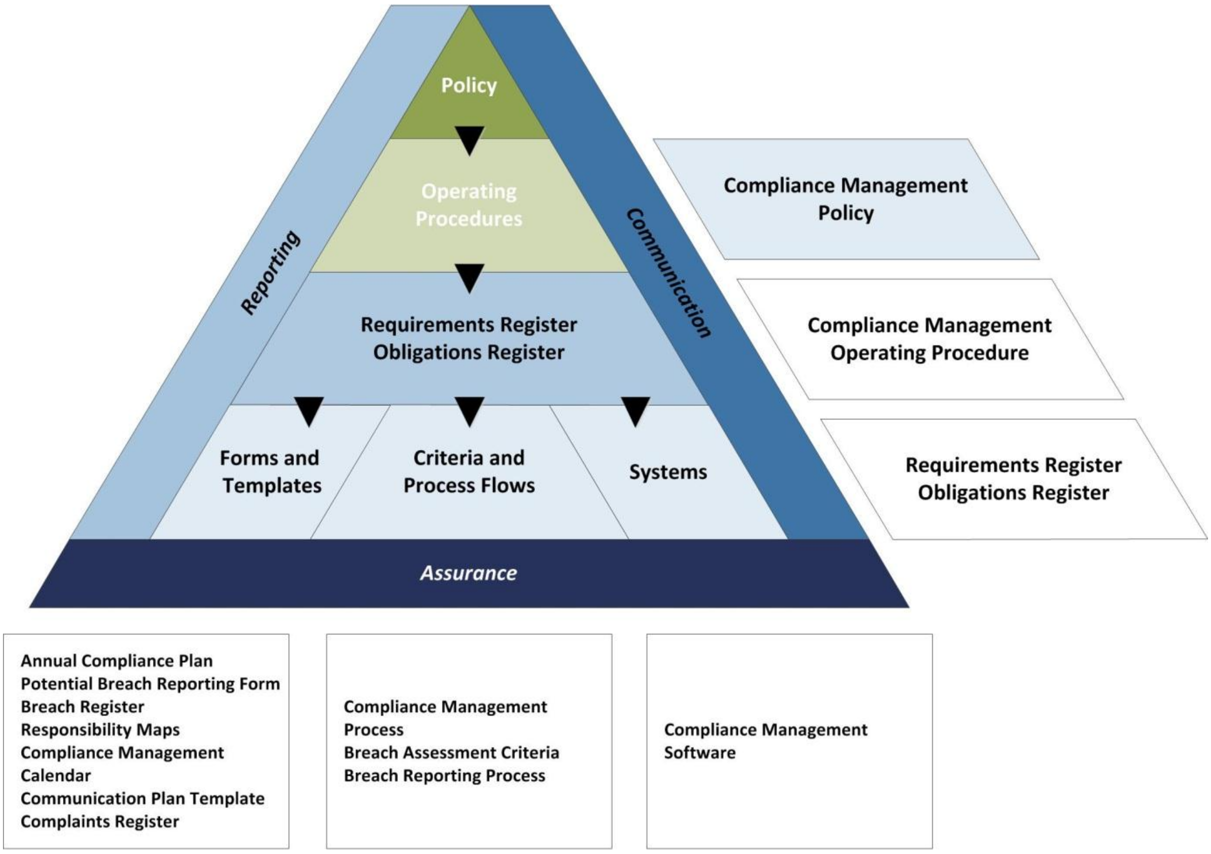
UNE's Compliance Policy (the Policy) is available on UNE's policy webpage. UNE's Compliance Framework (the Framework) and Procedures is set-out here and gives effect to the Policy. The Framework and Procedures are also available on UNE's webpage.

The success of the Framework relies heavily on the commitment and attitude of all employees and Management. UNE will not tolerate any instances of deliberate non-compliance.

Definition of Compliance

Compliance is defined in Australian Standard *Compliance programs,* AS3806-2006, as "Adhering to the requirements of laws, industry and organizational standards and codes, principles of good governance and accepted community and ethical standards."

The compliance management framework components are shown diagrammatically below:



Policy

Operating Procedures

Requirements Register
Obligations Register

Forms and Templates

Criteria and Process Flows

Systems

Reporting

Communication

Assurance

Compliance Management Policy

Compliance Management Operating Procedure

Requirements Register
Obligations Register

Annual Compliance Plan
Potential Breach Reporting Form
Breach Register
Responsibility Maps
Compliance Management Calendar
Communication Plan Template
Complaints Register

Compliance Management Process
Breach Assessment Criteria
Breach Reporting Process

Compliance Management Software

4. The Policy

The Compliance Policy D09/85794, sets out UNE's principles and responsibilities for compliance.

The Policy has been endorsed by the Audit and Risk Management Committee and approved by the Council on 02 November 2009. The policy is available on the UNE website.

The University is committed to good corporate governance practices and demonstrates its commitment to compliance by:

a) Support and endorsement from the UNE Council and Audit and Risk Committee for the University's compliance program.
b) The active engagement of the senior executive in the identification and management of compliance issues and risks.
c) The allocation of appropriate resources throughout the University to manage compliance obligations.

5. Risk Management

The key to compliance risk is to develop a systematic approach to managing compliance. AS/NZS ISO 31000:2009 Risk management – Principles and guidelines, is the standard that describes the systematic and logic process of risk management. It outlines how "Organizations of any kind face internal and external factors and influences that make it uncertain whether, when and the extent to which they will achieve or exceed their objectives. The effect this uncertainty has on the organization's objectives is "risk"." It is important to understand that "All activities of an organization involve risk. Organizations manage risk by anticipating, understanding and deciding whether to modify it. Throughout this process they communicate and consult with stakeholders and monitor and review the risk and the controls that are modifying the risk."

Enterprise risk management (ERM) is the practice of building an organisation-wide risk management program to identify, manage, mitigate and eliminate a diversity of risks – from compliance and political risks to financial and operational risks. Every organisation will have a different risk profile based on its business focus, geographical area of activity, regulatory environment and the type of business.

UNE compliance management will address the key strategic risk operational consequence areas:

1. Reputation
2. Market and Product Development
3. Financial Sustainability
4. Financial Systems
5. Human Resource Planning

7. IT Strategy and Infrastructure
8. Legal and Legislative Environment
9. Business Interruption
10. Government Policy Changes
11. Student Performance and Satisfaction

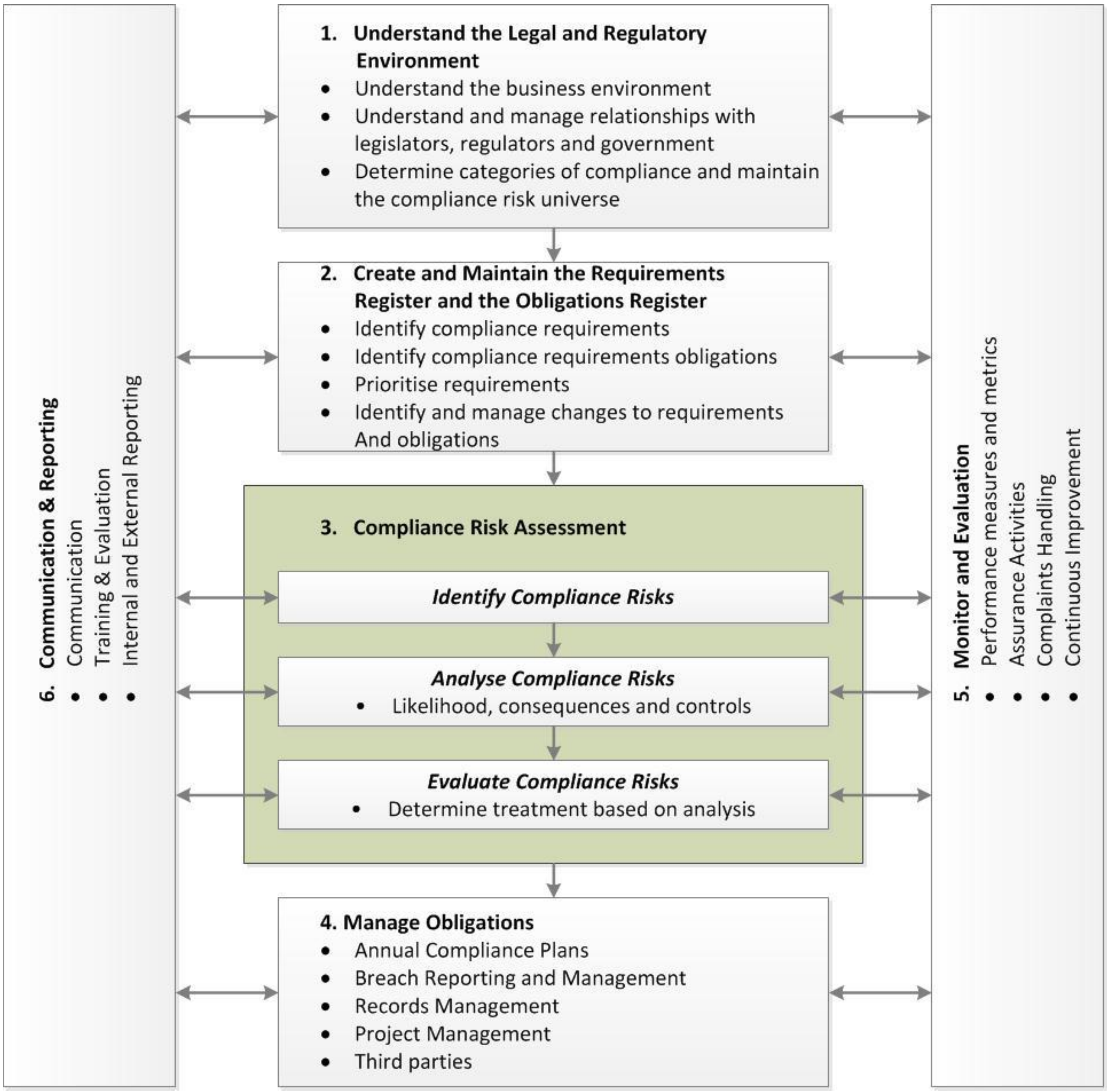
6. Project Management

12. International Economic, Political and Social Environment

6. Compliance Management Process

Compliance management uses the ***Australian Standard for Compliance Programs (AS 3806-2006)*** as the basis for the framework. All compliance management processes must follow this framework.

The diagram below depicts the six main phases of the compliance management process:



1. Understand the Legal and Regulatory Environment
- Understand the business environment
- Understand and manage relationships with legislators, regulators and government
- Determine categories of compliance and maintain the compliance risk universe
2. Create and Maintain the Requirements Register and the Obligations Register
- Identify compliance requirements
- Identify compliance requirements obligations
- Prioritise requirements
- Identify and manage changes to requirements And obligations
3. Compliance Risk Assessment
Identify Compliance Risks
Analyse Compliance Risks
- Likelihood, consequences and controls
Evaluate Compliance Risks
- Determine treatment based on analysis
4. Manage Obligations
- Annual Compliance Plans
- Breach Reporting and Management
- Records Management
- Project Management
- Third parties
5. Monitor and Evaluation
- Performance measures and metrics
- Assurance Activities
- Complaints Handling
- Continuous Improvement
6. Communication & Reporting
- Communication
- Training & Evaluation
- Internal and External Reporting

Procedures for managing compliance are documented in the **Compliance Management Operating Procedures** document attached to this Framework. Compliance management must be performed in accordance with these operating procedures**.**

7. Responsibility and Accountability Structure

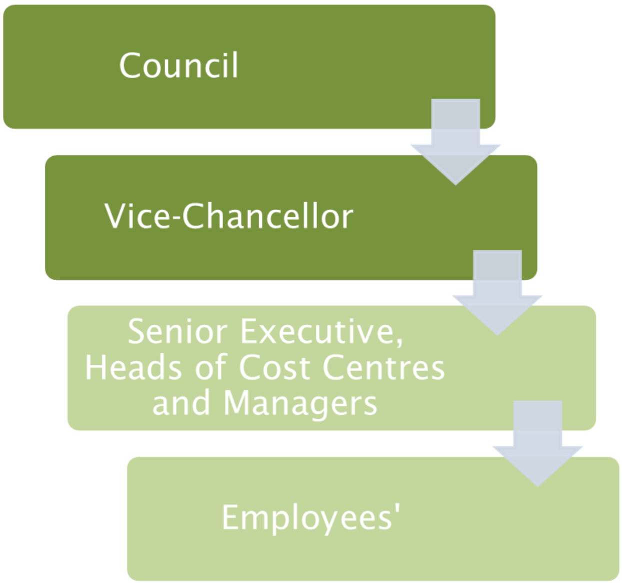
Under the University's Code of Conduct all staff members have a responsibility to the University to "comply with any relevant legislative, industrial and administrative requirements". In addition, certain individuals and groups across the University have specific responsibilities they are expected to undertake. These are described below.

7.1 Overview

The Council has ultimate accountability for approving the compliance management framework and the Vice-Chancellor has ultimate responsibility for ensuring an effective compliance management framework and procedures are operating.

All employees of the University have a responsibility to undertake their duties in accordance with the Framework and Procedures. The most important factor to ensure success of the Framework is the commitment and attitude of all employees.

The responsibility structure for compliance management is depicted by:



Council

Vice-Chancellor

Senior Executive, Heads of Cost Centres and Managers

Employees'

7.2 Council

Council is accountable for determining the compliance management framework, maintaining an effective compliance management capability, and ensuring that all compliance risks associated with the University's objectives are effectively managed.

The Council is responsible for:

- Approving the Policy.
- Overseeing and monitoring risk management and risk assessment across the University, and therefore compliance management as it is a foundation component of the risk management framework.

- Approving and monitoring systems of control and accountability for the University.
- Establishing policies and procedural principles for the University consistent with legal requirements and community expectations.

7.2.1 Audit and Risk Committee

Gives advice to Council on:

- Compliance of UNE and related entities to laws and regulations, including those relating to governance, audit, risk management, the environment, employment practice and anti-discrimination.
- Procedures, programs and policies of the University relating to compliance.
- Risk management and risk assessment across the University.
- Systems of control and accountability for the University.

Is responsible for:

- Reviewing whether management has in place a current and appropriate 'enterprise risk management' process, and associated procedures for effective identification and management of the University of New England's financial and business risks.
- Determining whether management has appropriately considered legal and compliance risks.
- Reviewing the effectiveness of the system for monitoring the University of New England's compliance with applicable laws and regulations, and associated government policies.

7.3 Vice-Chancellor and CEO

The Vice-Chancellor (VC) has ultimate responsibility for ensuring there is an effective Compliance Management Framework and operating procedures in place. The VC is accountable for regular reviewing of the adequacy of the framework in managing compliance and reporting any significant compliance breaches to the Audit and Risk Committee.

Is responsible for:

- Approving the Framework and Procedures.
- Ensuring managers and employees are aware of their responsibilities under the Framework.
- Ensuring managers and employees are aware that deliberate non-compliance will not be tolerated.
- Ensuring an effective risk management system is operating.
- Ensuring appropriate cost effective internal control systems are in place.
- Ensuring identified compliance risks are fully addressed.
- Receiving reports on high and above risk non-compliance areas and breaches and approving any further action plans.

7.4 Executive Management

Executive Management is ultimately responsible for the effective management of, and compliance with, all applicable regulatory and business compliance requirements of the University including ensuring all breaches are managed and reported appropriately.

Executive management are responsible for:

- Taking a leadership role in promoting a culture of compliance management and control in their area of responsibility.
- Ensuring implementation of the Framework and Procedures.
- Ensuring effective risk management.
- Ensuring internal control systems are operating.
- Ensuring employees are aware of the Policy, Framework and Procedures and their responsibilities as part of the Framework and Procedures.
- Implementing the Policy, Framework and Procedures within their area.
- Identifying risks and developing appropriate internal control systems to mitigate those risks.
- Considering new and emerging risks on a regular basis and where necessary adjusting systems for control of these risks.
- Ensuring employees understand the purpose of internal controls.
- Ensuring employees are complying with internal controls.

7.5 Managers

Managers are responsible for ensuring compliance with all regulatory and business compliance requirements and obligations associated with the activities of their position including identification, reporting and managing any compliance breaches.

Specific responsibilities for managing compliance include:

- Promoting a culture of compliance management and control in their area of responsibility.
- Managing compliance in accordance with the Compliance Management Operating Procedures.
- Identifying compliance requirements and obligations.
- Maintaining Compliance Obligations Register/s.
- Developing and communicating the Annual Compliance Plan.
- Ensuring employees are adequately trained in compliance obligations relating to their position and that training is up to date.
- Ensuring compliance is factored into position descriptions and performance management processes.
- Ensuring compliance capabilities and performance is factored into contracts with external customers and suppliers.
- Reporting, managing and resolving breaches.
- Adhering to records management policies and procedures.

7.6 Audit and Risk Directorate (ARD)

The ARD are responsible for ensuring that the compliance management framework is appropriate, effective and utilised in managing the risks of the University, and that the status of UNE's compliance obligations is regularly monitored, reviewed and reported to Management and the Audit and Risk Committee.

Key responsibilities include:

- Developing and maintaining the Compliance Management Policy, Framework and operating procedures, making sure that expectations for managing compliance are properly documented, readily available to and clearly understood by relevant management and employees.
- Continually reviewing and assessing the appropriateness and effectiveness of the Compliance Management Framework in identifying and managing compliance obligations.
- Regularly reporting on compliance management issues and any breaches to Management and the Audit and Risk Committee.
- Promoting a culture of compliance management and control throughout UNE.
- Communicating and implementing the Compliance Management Framework and Policy across UNE.

7.7 Employees

Every employee is responsible for ensuring their own compliance with all regulatory, legislative and internal policies and procedures associated with the activities of their position, including identification, management and reporting of any compliance breaches.

In addition, employees are responsible for attending scheduled compliance training, and reporting and escalating any compliance concerns, issues and failures in accordance with the Breach Reporting Process.

8. Reporting Responsibilities

8.1 Annual Reporting

Each Manager is required to complete and sign-off an Annual Compliance Plan (See Attachment E of the Compliance Management Operating Procedures document) for their area of responsibility; this details for their area:

- Any compliance requirements and/or obligations impacting on their school/directorate/unit.
- Annual reporting requirements for these areas of responsibility.
- Annual mandatory audit requirements for these areas of responsibility.
- Annual training requirements for these areas of responsibility.

8.2 Obligations Register

All Heads of Schools/Directors/Managers are responsible identifying the compliance requirements (both regulatory and business) associated with their activities, and identifying, documenting and understanding the key obligations under each of the compliance requirements for which they have operational responsibility and documenting these in the Compliance Obligations Register (procedures, Attachment C). The Compliance Obligation

Registers should be completed for all compliance requirements; updated as required; and reviewed annually.

8.3 Breach reporting and management

Compliance breaches must be reported and managed in accordance with the Breach Reporting Process and assessed utilising the Breach Assessment Criteria.

The level to which breaches are to be reported is detailed below:

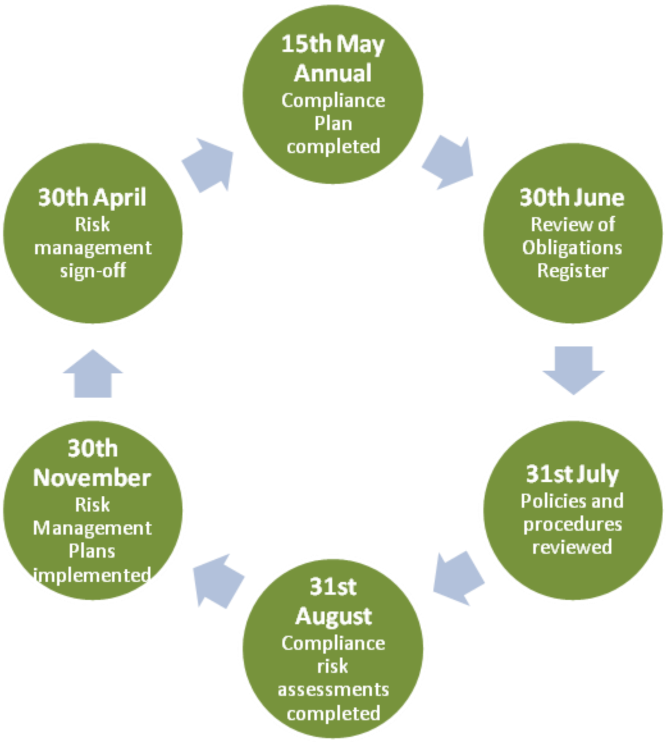
	Breach Rating				
Reporting Requirements	Very High	High	Medium	Low	Very Low
Audit and Risk Committee	√	√			
Vice-Chancellor / CEO	√	√	√		
Executive Management	√	√	√	√	inform
ARD Director	inform	inform	inform	inform	inform

8.4 External Reporting Requirements

Each manager is responsible for completing and lodging the reporting requirements for the compliance requirements or obligations which fall under their area of responsibility, by the required date, to required party with the appropriate level of internal approval.

9. Annual Compliance Management Calender

This document is used by Managers to document and diarise all their annual activities associated with their areas of compliance responsibility. These include completion of compliance plans, reviews of requirements and obligations, policy and procedure updates, risk assessments, reporting, training and assurance activities.


15th May Annual Compliance Plan completed
30th June Review of Obligations Register
31st July Policies and procedures reviewed
31st August Compliance risk assessments completed
30th November Risk Management Plans implemented
30th April Risk management sign-off

Month	Activity	Requirement	Responsibility
May	Complete Annual Compliance Plan	Compliance Policy	
June	Review and update Compliance Obligations Register for changes in legislation/regulations	Compliance Policy	
July	Update all policies and procedures to reflect changes in obligations	Compliance Policy	
August	Complete Compliance Risk Assessment	Compliance Policy	
September			
October			
November	Implement compliance risk management plans		
December			
January			
February			

March			
April	Self-assessment on operation of controls managing compliance risks	Compliance Policy	

Other Directorate/Unit/School specific activities (taken from the Annual Compliance Plan) to be incorporated into the Compliance Management Calender include:

- External reporting requirements
- External audit/assurance requirement
- Training requirements

Section 2 : Compliance Management Operating Procedure

1. Application

This operating procedure applies to all employees and should be used in conjunction with the Compliance Policy and the other components of the Compliance Management Framework.

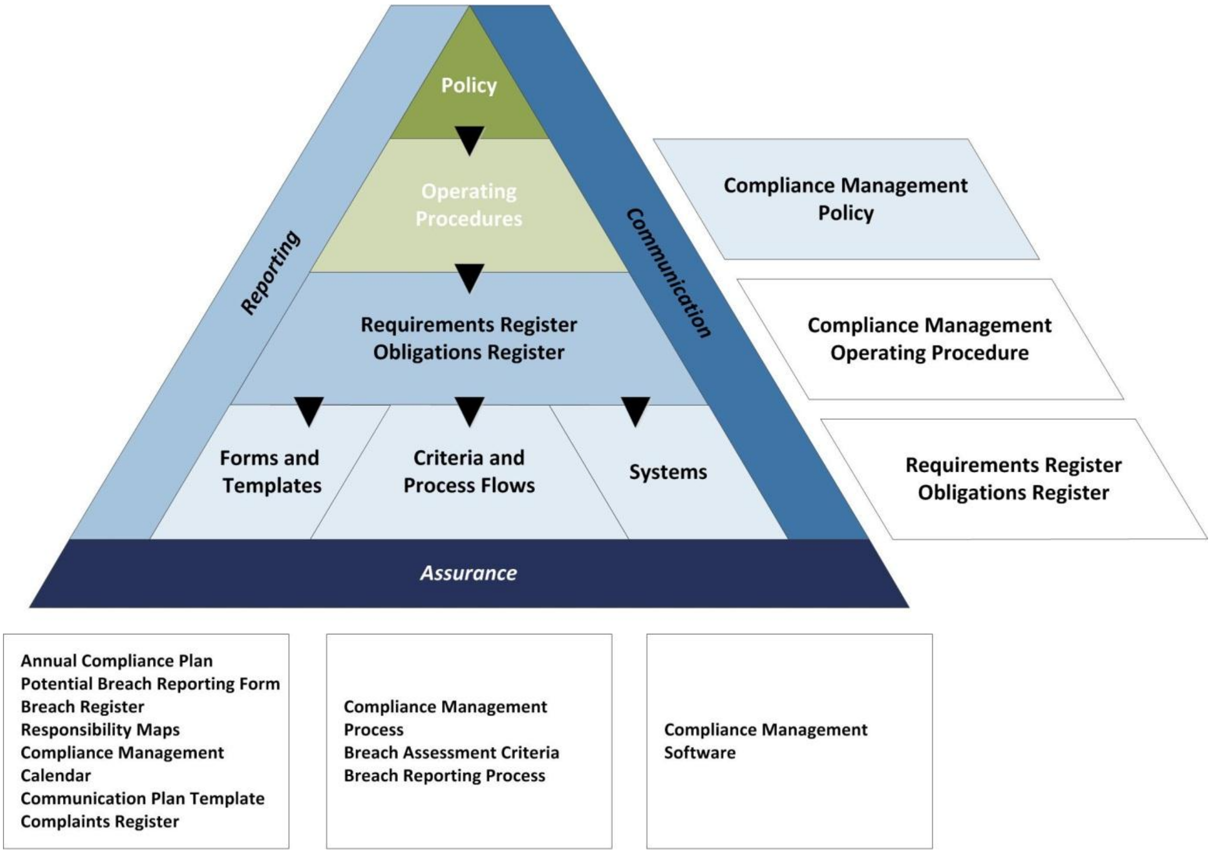
Exclusions

Compliance framework and procedures falling within the portfolio of the Academic Board are outside the scope of this procedure, except for, the provisions contained within section 3.6.4, Reporting, of the Compliance Management Procedures.

2. Purpose

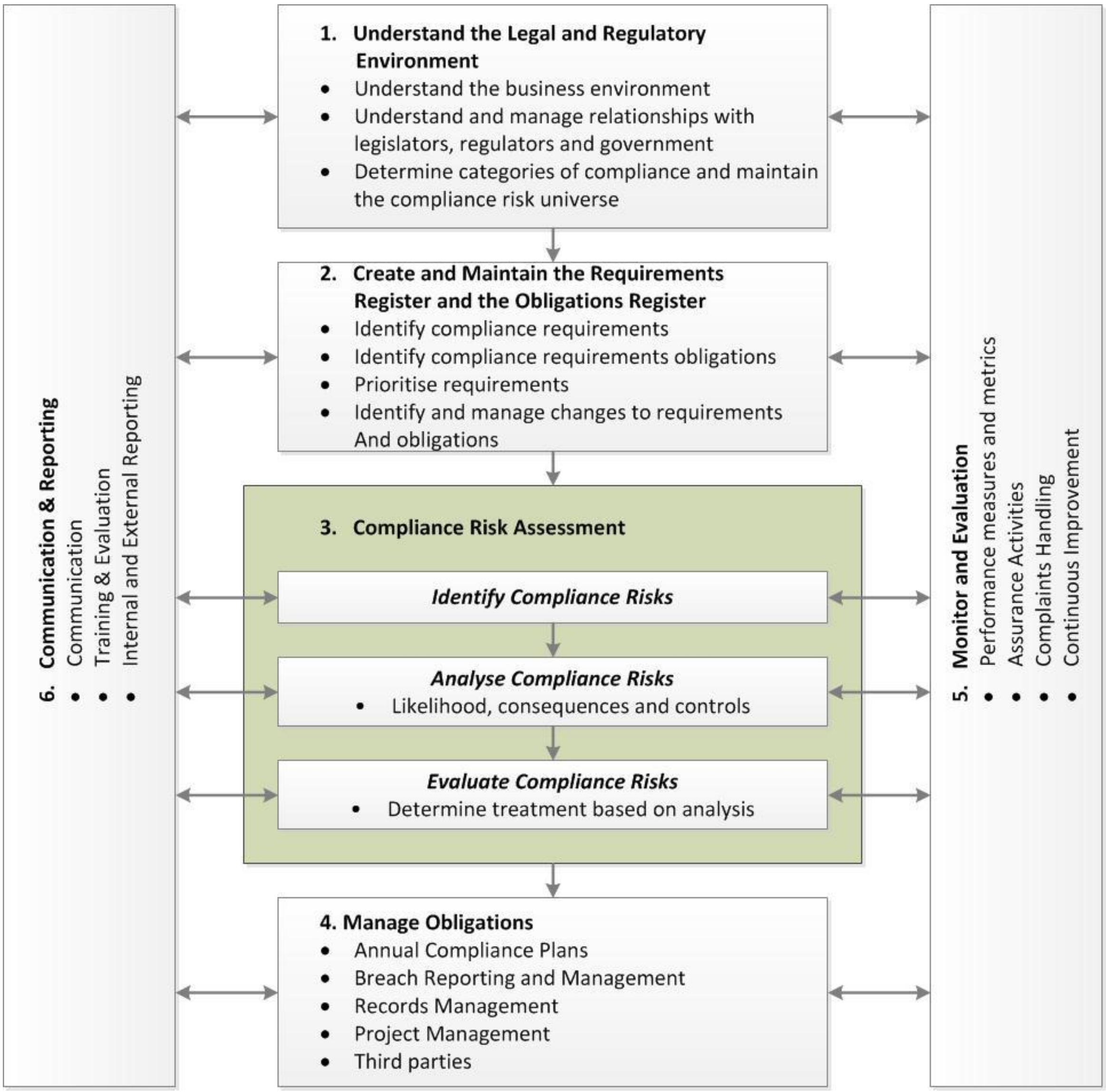
The Compliance Management Operating Procedure (the Procedure) is a key component of the Compliance Management Framework and articulates how the Compliance Management Policy is to be implemented, how compliance management processes are to be carried out and the associated accountabilities for carrying out each stage of the process.

The associated Compliance Management Framework components are as follows:


Policy
Operating Procedures
Requirements Register
Obligations Register
Forms and Templates
Criteria and Process Flows
Systems
Reporting
Communication
Assurance
Compliance Management Policy
Compliance Management Operating Procedure
Requirements Register
Obligations Register
Annual Compliance Plan
Potential Breach Reporting Form
Breach Register
Responsibility Maps
Compliance Management Calendar
Communication Plan Template
Complaints Register
Compliance Management Process
Breach Assessment Criteria
Breach Reporting Process
Compliance Management Software

3. The Compliance Management Process

The diagram depicts the six main phases of the compliance management process:



1. **Understand the Legal and Regulatory Environment**
   - Understand the business environment
   - Understand and manage relationships with legislators, regulators and government
   - Determine categories of compliance and maintain the compliance risk universe

2. **Create and Maintain the Requirements Register and the Obligations Register**
   - Identify compliance requirements
   - Identify compliance requirements obligations
   - Prioritise requirements
   - Identify and manage changes to requirements And obligations

3. **Compliance Risk Assessment**

Identify Compliance Risks

Analyse Compliance Risks
- Likelihood, consequences and controls

Evaluate Compliance Risks
- Determine treatment based on analysis

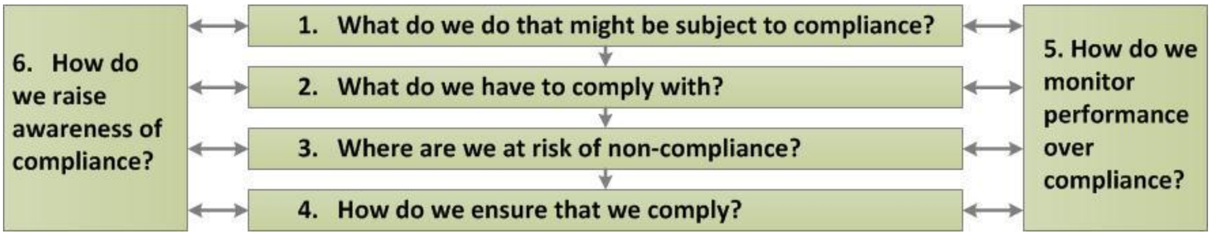
4. **Manage Obligations**
   - Annual Compliance Plans
   - Breach Reporting and Management
   - Records Management
   - Project Management
   - Third parties

5. **Monitor and Evaluation**
   - Performance measures and metrics
   - Assurance Activities
   - Complaints Handling
   - Continuous Improvement

6. **Communication & Reporting**
   - Communication
   - Training & Evaluation
   - Internal and External Reporting

Each phase of the compliance management process is explained in this operating procedure, which is accompanied by forms and templates to guide the compliance management process for UNE.

In simple terms the process can be described by the following questions:



1. **What do we do that might be subject to compliance?**
2. **What do we have to comply with?**
3. **Where are we at risk of non-compliance?**
4. **How do we ensure that we comply?**
5. **How do we monitor performance over compliance?**
6. **How do we raise awareness of compliance?**

3.1 Understand the Legal, Regulatory and Business Environment

Responsible Officer/s	Responsibilities
Executive Management	• Each member of the executive team should understand the environment the University operates in, and the compliance requirements of the University as a whole.
Head of School/ Director / Manager	• Each manager should understand the environment they operate in and thus the processes, systems, assets, people, or industry affiliations within their area of responsibility that are subject to compliance requirements. (NB. Universities are in the public sector and will thus have additional compliance requirements imposed by State Government, in addition to those already imposed by Federal Government or any specific industry bodies). • Each manager needs to have an understanding of the regulators, legislators and government bodies which monitor or administer the compliance requirements in their area of responsibility. Knowledge of these organisations can be gained through internal research, via the internet and through professional networks, and once identified, a process for engaging with these organisations on an ongoing basis should be implemented to increase awareness of the following: o Upcoming and initiated changes to legislation, regulations and directives. o Focus areas of the regulator or government agency which may result in assurance activity. o Availability of training or educational materials. o Reporting requirements or deadlines. o Assurance requirements. o The relevant legislator, regulator or administrator for each compliance requirement should be documented in the centrally held Compliance Obligations Register (Attachment C), along with the key contacts at these organisations their contact details documented • Identifying changes to the Compliance Risk Universe and communicating these to the Audit and Risk Directorate.
Audit and Risk Directorate	• Centrally maintaining an up to date Compliance Risk Universe and ensuring it is accessible.

3.1.1 Determine Categories of Compliance and Maintain a Compliance Risk Universe

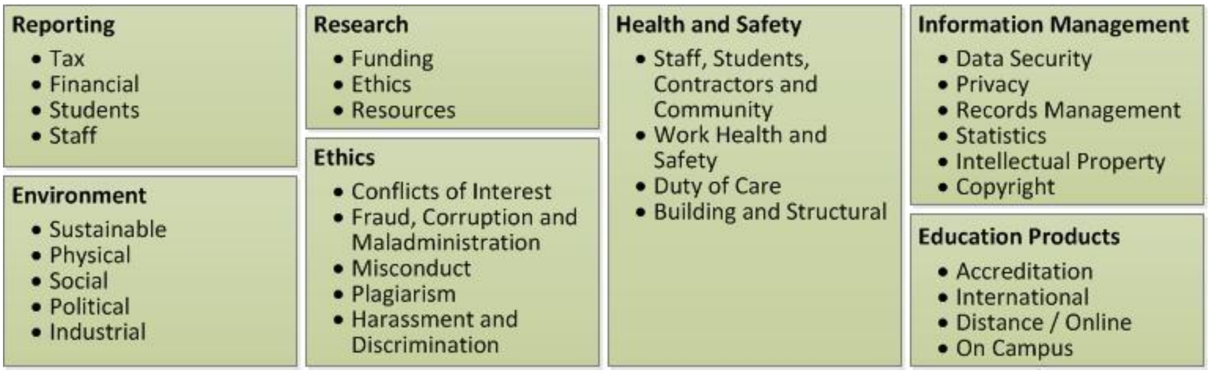
Once the business, legislative and regulatory environment have been understood and identified, the categories of compliance should be determined based on the activities in the University subject to compliance, and hence the risk of non-compliance. These categories of compliance are also what is known as the "Compliance Risk Universe", and represent the sources of risk of non-compliance facing the University. The categories of compliance in the risk universe incorporate both regulatory and business compliance requirements. The key purposes of the Compliance Risk Universe are as follows:

- Use as a basis for compliance risk assessments.
- To prioritise allocation or resources for managing compliance.

- Identify areas of responsibility and enable allocation of responsibility to business areas.

The Compliance Risk Universe is dynamic and will evolve over time as new compliance requirements are identified and others cease to exist. To support this evolution, the Compliance Risk Universe should be reviewed on an annual basis to incorporate any emerging areas of compliance risk or any areas that are no longer a focus for the organisation.

The following is an example of a Compliance Risk Universe:



Reporting
- Tax
- Financial
- Students
- Staff

Environment
- Sustainable
- Physical
- Social
- Political
- Industrial

Research
- Funding
- Ethics
- Resources

Ethics
- Conflicts of Interest
- Fraud, Corruption and Maladministration
- Misconduct
- Plagiarism
- Harassment and Discrimination

Health and Safety
- Staff, Students, Contractors and Community
- Work Health and Safety
- Duty of Care
- Building and Structural

Information Management
- Data Security
- Privacy
- Records Management
- Statistics
- Intellectual Property
- Copyright

Education Products
- Accreditation
- International
- Distance / Online
- On Campus

3.2 Create and Maintain Compliance Requirements and Obligations Registers

In order to be able to mitigate the risk of non-compliance and appropriately prioritise and allocate resources to manage compliance, there needs to be knowledge and understanding of the specific compliance requirements and obligations to which the organisation must adhere to.

Responsible Officer/s	Responsibilities
Executive Management	• Reviewing and approving all prioritisation/risk ratings. • Work with the Head of School/ Director / Unit Manager, the Director Audit and Risk Directorate, and other impacted areas to evaluate the impact of significant changes (Significant changes could impact on the processes of more than one area).
Head of School/ Director / Manager	• Identifying the compliance requirements (both regulatory and business) associated with their activities and informing ARD. • Identifying, documenting and understanding the key obligations under each of the compliance requirements for which they have operational responsibility and documenting these in the Compliance Obligations Register (Attachment C). • Filing all documents with ARD at email risk.mgt@une.edu.au • Prioritising all compliance requirements in their area of responsibility. • Identifying changes to compliance requirements and obligations for which they are responsible, on a timely basis and implementing the required changes to ensure the University continues to comply with its obligations. ○ Informing and discussing with Executive Management all potential significant changes, such as the introduction of a new regulation or legislation. ○ Communicating changes to ARD, as and when they occur. ○ Communicating changes to the relevant stakeholders.
Audit and Risk Directorate	• Centrally maintaining an up to date Compliance Requirements Register and ensuring it is accessible to all Managers. • Ensuring the central Compliance Requirements Register is updated for any communicated changes.

3.2.1 Compliance Requirements

A ***compliance requirement*** is a law (legislated or common law), regulation, government directive, industry code or standard, permit, licence, contract or internal policy/procedure that the University must comply with.

Compliance requirements can either be:

- Regulatory (legal, regulatory, licence, contractual, permit or accreditation standards) compliance requirements; or
- Business (Internal Policy or “best practice" standards) compliance requirements

Compliance requirements can be identified through:

- Regular communication with the legislators and regulators
- Communication with industry bodies
- Professional associations and memberships
- Knowledge of the business and operating environment
- Internal communication
- Research

3.2.2 Compliance Requirements Register (Attachment B)

All compliance requirements are documented in a central Compliance Requirements Register which is administered by the Audit and Risk Directorate (ARD).

The Compliance Requirements Register will be used to populate the Annual Compliance Plan (see Section 4 and Attachment D) which describes the annual compliance responsibilities and activities for each area.

3.2.3 Compliance Obligations Register (Attachment C)

A compliance obligation is the specific action within a requirement that the University must undertake in order to comply with the overarching compliance requirement.

NB: Where compliance management software is used, requirements and obligations registers will be maintained within the software.

3.2.4 Identifying and Managing Regulatory and Legislative Changes

There are a number of methodologies that can help areas identify and manage regulatory and legislative changes. Some of these include:

- Subscribe to legislative and regulatory updates provided by government, regulators and other sources.
- Subscribe to information services from external providers including regulators, legal firms, industry associations and professional research groups.
- Facilitate working groups with relevant areas within the University and industry groups to interpret, coordinate and implement legislative change requirements.
- Build constructive and transparent relationships with the relevant regulatory and government bodies.
- Manually monitor key information sources such as government, regulator and legal websites.

Fees for subscription services essential to managing a high priority and/or complex compliance requirement should be budgeted for annually.

Process upon Identification of any Regulatory or Legislative Change:

1. Identify the requirement and obligations that have changed, been added or been removed.
2. Identify the processes impacted by the change.
3. Determine the magnitude of the change (i.e. Minor or Significant).
4. Implement procedures as appropriate based on the magnitude of the change (see below.)

i) Minor Changes

Minor changes are defined as "Alterations to existing ***compliance requirements*** that will have a minimal impact on the University's processes. For example; small changes to the wording of ***obligations*** that have little or no effect on operating processes, or amendments to minor *obligations* within a requirement that have little impact on how processes are performed."

In the event of a minor change;

Update:

- Compliance Obligations Register
- Responsibility Map (if required)
- Policy and procedure documents (if required)
- Operational processes (if required)

Communicate:

- Details of the change to the staff involved in the operational processes affected, through training or other appropriate means.
- Confirmation to Senior Management and the Director Audit and Risk that all the required amendments have been made.

ii) Significant Changes

Significant changes are defined as "Changes to compliance requirements that are likely to have a significant impact on the organisation's processes. For example, the introduction of new laws, regulations or, changes to or the introduction of new ***obligations*** in existing ***requirements***, that would cause a fundamental change in an operating process."

Significant changes, if brought about by the introduction of a new compliance requirement will often require full scale implementation of the ***compliance management framework.***

In this case, the process will be as follows:

1. Compile a Compliance Obligations Register (Attachment C) for the requirement.
2. Determine the priority of the Requirement using the Prioritisation Considerations.
3. Notify other schools/directorates/units with responsibilities for obligations.
4. Complete a Risk Assessment on the requirement (Level 1& 2 priority requirements only).

5. Ensure Annual Compliance Plans (Attachment D) are updated appropriately for the new requirements (all priority levels).
6. Update Annual Compliance Calendar (Attachment E) as appropriate.
7. Write new policies and procedures or update existing policies and procedures for the new obligations.
8. Train all staff with involvement in processes affected by the new requirements, in their responsibilities and any changes to current processes.

3.3 Compliance Risk Assessment - Identify, Analyse and Evaluate Compliance Risks

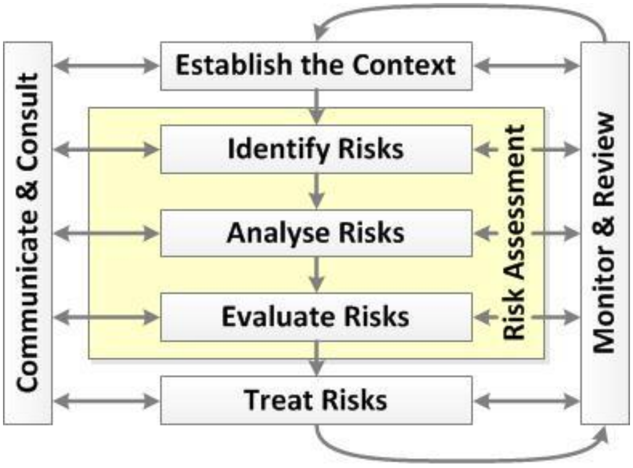
A risk is a set of circumstances that hinder the achievement of objectives.

In the case of a compliance risk, the objective is adhering to compliance obligations, and thus compliance risk is; "the likelihood of something happening that could prevent the organisation from complying with its obligations".

Responsible Officer/s	Responsibilities
Executive Management	• Risk identification. • Performing an annual assessment over the risk of non-compliance in their area of responsibility. • Documenting those risks and managing and reporting them in accordance with the Risk Management Policy and Guidelines. • Determine the level and type of treatment required to mitigate the risk and develop a risk management plan
Head of School/ Director / Manager	• Performing an annual assessment over the risk of non-compliance in their area of responsibility. • Documenting those risks and managing and reporting them in accordance with the Risk Management Policy and Guidelines. • Determine the level and type of treatment required to mitigate the risk and develop a risk management plan.
Audit and Risk Directorate	• Providing the risk management framework, tools, systems and support to enable the University to manage its compliance risks effectively.

3.3.1 Risk Management Process

Risk Management within an organisation can be performed in accordance with AS/NZS ISO 31000:2009 - Risk management – Principles and guidelines:



For further information on Risk Management see the Risk Management Policy and Guidelines.

Compliance Risk Assessments

Compliance risk assessments can be focused on categories of compliance obligations or requirements listed in the Compliance Risk Universe. However the risk universe is a tool for guidance only so risk assessments can be performed on other compliance areas if appropriate.

The compliance risk assessment should be performed using the processes, systems and tools outlined in the University's Risk Management Policy and Guidelines.

In summary, the major steps of this process are as follows:

- Identify Risks
  Identifying where the University is at risk of non-compliance and what would be the potential causes of non-compliance.

- Analyse the Risks (Assess Likelihood and Consequence)
  Determine how likely it is that non-compliance will occur and what is the consequence if it does.

- Evaluate the Risk
  Determine the level and type of treatment required to mitigate the risk and develop a risk management plan.

Risk treatment plans involve selecting one or more options for modifying the risk, and implementing those options. Once implemented, treatments provide or modify the controls that will either reduce the likelihood of a risk occurring or reduce the consequence or impact if it does occur.

Risk treatment plans should be developed and implemented for all risks rated 'Medium' or above, where controls are not fully operational, in line with the Risk Management Policy and Guidelines.

Risk Reporting and Assurance Requirements
The process for assessment and management of compliance risks should be in line with the University's Risk Management Policy and Guidelines. and hence the reporting and assurance requirements for compliance risks follow that of any other risk.

3.4 Manage Obligations

Managing compliance extends further than reporting compliance to legislators and regulators; it is about educating and raising awareness, ensuring our processes facilitate compliance, ensuring accountability for compliance and providing a mechanism for reporting and handling breaches and incidents.

Responsible Officer/s	Responsibilities
Executive Management	• Considering compliance requirements and obligations in the planning phase of any project, and managing compliance obligations throughout the course of the project.
Head of School/ Director / Manager	• Completing and signing off an Annual Compliance Plan (Attachment D) documenting their, compliance responsibilities; reporting, assurance and training requirements; and details of compliance risks rated 'Medium' or above, for the compliance obligations impacting on the operations of that area. Sign-off of this plan is acknowledgement that the School/Directorate/Unit recognises the compliance requirements and obligations affecting the processes of their area, that they will effectively manage the risks around meeting those requirements or obligations, and that they will complete any reporting, assurance or training responsibilities associated with those compliance requirements or obligations. • Reporting potential breaches in accordance with the breach reporting process and implementing required breach remediation procedures. • Ensuring all reported potential breaches are escalated and managed in accordance with the breach reporting policy and process. • Following the reporting of a breach or a potential breach, the manager responsible should use the incident as an opportunity to identify the potential weakness in current processes that enabled the incident to occur in the first place, and also those areas in which to make process improvements. • Process improvements required resulting from a breach should be recorded in the Breach Reporting Form (Attachment G) • Considering compliance requirements and obligations in the planning phase of any project, and managing compliance

Responsible Officer/s	Responsibilities
	obligations throughout the course of the project.
Audit and Risk Directorate	• Ensuring annual compliance Plans are completed and centrally filing all completed plans.

3.4.1 Annual Compliance Management Calendar (Attachment E)

The Annual Compliance Management Calendar in Attachment E provides a tool whereby a school/directorate/unit can diarise and organise all their compliance management activities throughout the year, including any reporting, assurance, training, risk management or internal sign-off processes.

3.4.2 Reporting Potential Breaches of Compliance Requirements

A breach is defined as "an act or omission whereby the University has not met its compliance obligations, processes or behavioural obligations".

Schools/ Directorates/Units are at the forefront of compliance management and are likely to be the origination of the reporting of potential breaches. Potential breaches can be identified from a number of sources, these include:

- Fines, penalties, damages or legal costs.
- Local, State, national or international adverse or unwanted publicity or media attention.
- Inquiry from Audit Office of NSW, Tertiary Education Quality and Standards Agency (TEQSA) or other Government body.
- Allegations of wrong doing, complaints from stakeholders or whistleblowing reports.
- Death, injury or disability.
- WH&S incidents (it should be noted that the incident itself is not a breach and incidents can occur that are not associated with a compliance breach.)
- Industrial action or union activity
- Loss of staff morale.
- Enforcement action or inquiry by a Regulator or other Government authority.
- Criminal prosecution of the University, Executive or individual staff.
- Public allegations and/or civil claims relating to our corporate/business character, image or reputation.
- Outcomes from audit and assurance processes.
- Systemic errors / problems.
- Detailed breach indicators and reporting criteria are contained in Attachment J.

The process for investigating, managing and reporting on potential breaches is included in Attachment I, and is an obligation under the Compliance Management Policy and must be utilised for managing all breaches.

All potential breaches must be recorded on the Potential Breach Reporting Form in Attachment G, and all confirmed breaches must be recorded on the Breach Register in Attachment H.

3.4.3 Records Management

Accurate up-to-date records of our compliance activities will be maintained to assist in the monitoring and review process and demonstrate conformity with the Compliance Management Framework. Record-keeping will include recording and classifying complaints, disputes and alleged compliance failure and the steps taken to resolve them. Records must be stored and managed in accordance with the Records Management Policy.

3.4.4 Compliance and Project Management

Compliance requirements and obligations should be understood and managed on all projects. In particular:

- In the planning phase of all projects an assessment of all the compliance requirements that may impact on the project, must be made. The Compliance Risk Universe should be used to assist in this process to identify the categories of compliance that could be applicable to the project.
- All compliance requirements identified should be documented in the Project Brief.
- Obligations Registers for those compliance requirements should be reviewed and management plans for meeting all applicable obligations should be included in project plans.
- Compliance risks should be considered when conducting risk assessments during each phase of the project.

3.5 Continual Monitoring and Evaluation

For compliance management to be effective, performance of the compliance management processes should be continually monitored and measured. This includes the performance of individuals and schools/directorates/units in managing their own compliance obligations, but also the effectiveness, adequacy and appropriateness of the mechanisms used to manage compliance, i.e. the performance of the compliance management framework itself needs to be measured.

Performance can be measured through monitoring of achievement against defined key performance indicators (KPIs) or through internal or external assurance activities such as audits or reviews.

Responsible Officer/s	Responsibilities
Executive Management	• Managing the compliance performance of their faculty/area and reporting performance in line with the compliance KPIs. • Informing the Audit and Risk Committee of the status of reports by Heads of Schools/ Directors/ Managers on the compliance performance of their area in line with the compliance KPIs. • Executive Management, Heads of Schools and Directors are responsible for ensuring that internal audit staff have unrestricted access to all employees, records and property of UNE and are entitled to such information and explanations as they may require

Responsible Officer/s	Responsibilities
	for audit purposes.
Head of School/ Director / Manager	• Managing the compliance performance of their school/directorate/unit and reporting performance in line with the compliance KPIs. • Coordinating any required assurance activities and reporting the results. • Managers are responsible for ensuring that they implement any agreed recommendations from internal or external assurance processes by the agreed deadlines, and are also responsible for ensuring that process improvements identified as a result of any breaches or potential breaches are implemented. • Reviewing all complaints received from stakeholders as they can provide an early warning or indication of where the University may be in breach of its compliance obligations. As a result complaints should be closely monitored for indications of compliance breaches and these complaints should be logged using the form in Attachment K and reported to the relevant Head of School/Director/Manager and the Director ARD. • Reporting their individual area performance to the Vice-Chancellors committee, by means of measuring performance against predefined Key Performance Indicators (KPIs). • Make an annual self-assessment on the operating effectiveness of the internal controls managing all 'Medium' to 'Very High' risks in their area of responsibility. • Certain compliance requirements will require that audit or external reviews are carried out on a periodic basis. Where this is the case the Manager of the area with responsibility for that compliance requirement is responsible for ensuring that this takes place. • Reporting external assurance activities • Executive Management, Heads of Schools and Directors are responsible for ensuring that internal audit staff have unrestricted access to all employees, records and property of UNE and are entitled to such information and explanations as they may require for audit purposes.
Audit and Risk Directorate	• To ensure the compliance management framework is operating effectively at managing the obligations of UNE, its performance will be measured through internal audit review, which will assess its effectiveness, adequacy and appropriateness in managing compliance. This reviewed is to be included in the annual audit plan. • The Director ARD is responsible for co-ordinating all internal audit activities included on the Audit and Risk Directorate Operational

Responsible Officer/s	Responsibilities
	plan. Controls and mitigation strategies for compliance risks will be subject to internal audit review. From time to time compliance with certain requirements and obligations will be subject to internal audit to provide assurance internally that obligations are being managed effectively and to ensure compliance processes are being continually improved. • Coordinating the reporting on the status of any assurance findings or recommendations to the Audit and Risk Committee.

3.5.1 Performance Indicators

Examples of KPIs which can be used are as follows:

Example KPIs	Rationale
Individual School/ Directorate/Unit	
Number of confirmed *breaches*	The # of breaches should decrease with the # of areas actively managing compliance.
Development and completion of annual compliance plans	By developing and completing compliance plans areas are demonstrating their commitment to managing compliance.
Number of training sessions held. Staff attendance at mandatory training sessions	If staff are educated and have knowledge of their compliance responsibilities, compliance obligations will be more actively managed.
Number of management plans in place for compliance risks	By developing risk management plans, the likelihood of compliance failures occurring should be reduced.
Number of compliance requirements of area mapped to the Framework	The greater the number of compliance requirements mapped to the framework, the greater the assurance that compliance is being effectively managed.
Number of internal or external assurance findings	If compliance is being managed effectively and improvements continually made, the number of assurance findings should decrease.
Timeliness in remedying compliance breaches or assurance findings	Findings and process improvements should be made on a timely basis to effectively manage compliance.
Compliance Management Framework	
# of breaches and potential breaches reported from high priority compliance requirements	A successful framework will result in increased reporting and transparency.

Example KPIs	Rationale
Individual School/ Directorate/Unit	
# of confirmed *breaches*	A successful framework will reduce the amount of confirmed breaches.
Amount paid as a result of compliance breaches exceeding a particular threshold	A successful framework will reduce the amount paid in fines.
Decrease in the rating of compliance risks	A successful framework will improve the control structure and hence reduce the risk of compliance failure.
Alignment with AS3806 Compliance Management Standard or other best practices in compliance management	The framework should remain up to date with best practices in order to manage compliance effectively.

3.5.2 External Assurance Activities

Audit findings and recommendations

- The results of all assurance activities must be reported to the Director Audit and Risk, the Executive of that Directorate/ Faculty, and to the Audit and Risk Committee if required.
- In respect of any agreed findings or recommendations from assurance activities, Managers with responsibility for the associated obligations or processes impacted are responsible for ensuring that the finding is remedied by the agreed due date.
- Where the results of the assurance activity have been reported to the Audit and Risk Committee, progress in remedying assurance findings will be reported to the Committee on a regular basis.
- The results of all assurance activities should be used as part of the continuous improvement process for compliance management and be used as a mechanism to ensure that organisation’s processes are constantly progressed towards best practice.

3.5.3 Compliance Management Framework

Like other business processes, the Compliance Management Framework’s design and implementation will be subject to independent review so that the following can occur:

- Gaps in the compliance universe can be identified and improved.
- Education needs throughout the University can be identified and actioned.
- Potential and actual breaches can be understood, monitored, and reported and any other deficiencies or inefficiencies can be understood and resolved.

The Compliance Management Framework itself is therefore subject to review, including any component of the Framework, such as the Obligations Registers, Annual Compliance Plans, Risk Registers, Breach Register, Customer Complaints Register, and other related inputs and sources of information as required.

Reviews may be undertaken as part of:

- Management self-assessments
- Internal Audits
- External Audit; and
- Regulator or Other Audit

The results of these audits will feed into our continuous improvement processes for managing compliance, including the compliance control environment.

3.5.4 Continuous Improvement

Continuous improvement provides a mechanism to maintain a relevant and effective Compliance Management Framework. In this way continuous improvement serves to link potential or actual compliance failure with preventative of corrective action.

Compliance Management processes can be continuously improved through the following mechanisms:

- Implementing recommendations/findings from internal or external assurance processes.
- Reviewing compliance incidents, potential breaches or breaches to identify the causes.
- Reviewing and actioning customer and other stakeholder feedback or complaints.

3.6 Communications & Reporting

Responsible Officer/s	Responsibilities
Executive Management	• Ensuring that all stakeholders receive adequate communication on compliance requirements, responsibilities and performance.
Head of School/ Director / Manager	• Consider the type of compliance requirements and obligations for which they are responsible and develop a Communication Plan if a significant amount of communication to stakeholders is required to manage the obligations effectively. A Communication Plan should be developed to help ensure that the appropriate information is communicated on a timely basis, in the appropriate manner, to the appropriate stakeholders. • Ensuring that staff have the required level of competency to discharge their compliance obligations through ensuring compliance obligations are addressed in the University's training programs and their staff attend the appropriate training session(s). Specifically this includes: ○ Ensuring all new staff receive appropriate induction training ○ Ensuring ongoing staff training requirements are identified

	and scheduled on an annual basis ○ Monitoring staff attendance and performance at training ○ Ensuring training requirements are appropriately factored into the Performance Planning and Review process • Reporting breaches and potential breaches in line with the breach reporting process. • Reporting performance on compliance risks in line with the Risk Management Policy. • Completing and signing-off their annual compliance plan. • Reporting any changes to compliance requirements and obligations to the Director ARD. • Reporting the results of all assurance activities to the Director ARD.
All Staff	• Attend and participate in identified training.
Audit and Risk Directorate	• Ensuring all appropriate and relevant compliance activity is reported to the Audit and Risk Committee, including the status of any assurance finding or recommendations.

3.6.1 Communication

Managing compliance effectively requires continuous communication between internal and external stakeholders, and particularly with employees who have responsibility for processes subject to compliance obligations, and also regular reporting on the results of compliance management practices.

Communication is required to:

- Raise awareness and understanding
- Provide instruction
- Monitor performance
- Report performance
- Report breaches and incidents

Internal Stakeholders include employees (both permanent and casual), Executives, and Committees.

External Stakeholders could include relevant government bodies and organisations, students, outsource providers, contractors, suppliers, customers or regulatory bodies.

3.6.2 Communication Plans(Attachment F)

A communication plan would typically include:

- Description of the compliance obligation
- A description of the information to be communicated

- The purpose of the communication
- Identification of audience: who they are and whether they are internal or external stakeholders
- Type of communication method. Communication methods include:
  - Compliance training
  - The intranet
  - Management and Committee meetings
  - Posting items on the wall in highly frequented areas
  - Reporting processes
  - Leading by example
  - Mentoring; and
  - Questionnaires
- Frequency or timing of communication
- Expected response or level of stakeholder involvement (if applicable)

3.6.3 Training & Education

All staff have compliance obligations and should be competent to discharge these effectively. Competence can be attained through education, training or work experience. Training or education could include:

- Induction
- Internal or external training on specific areas of compliance
- Internal training on policies and procedures
- On the job training
- External training held by legislators, regulators, standard setters, consultants or other service providers
- Accreditation programs
- Professional qualifications or certifications
- University degrees or diplomas

Annual training requirements should be documented in the Annual Compliance Plan for each area. See Attachment D.

3.6.4 Reporting

The format, content and timing of internal compliance reporting, unless prescribed by law, is tailored to the nature of the issue being reported as per the following guidelines:

- Incidents and potential breaches are reported as and when they occur, to Head of Schools/ Directors/Managers, and where appropriate escalated to Executive Management and the Director Audit and Risk, as per the Breach Reporting Process in Attachments G – J.
- Reporting on performance for Compliance risks is as per the Risk Management Policy.
- The Annual Compliance Plan will be reported and signed-off at the start of each year per the template at Attachment D.
- Changes in compliance requirements and obligations should be reported to the Director Audit and Risk as and when they occur.

- Results of assurance activities are reported to the Director Audit and Risk, Executive Management and the Audit and Risk Committee as required.
- During the year, compliance issues will be reported as required on an adhoc basis in:
    - Executive Meetings
    - Committee Meetings
    - Management Meetings
    - Audit and Risk Committee Meetings

Attachment A – Definitions

Term	Definition
Assurance	A positive confirmation intended to give confidence that what is reported may be relied upon.
Assurance Services	An objective examination of evidence for the purpose of providing an independent assessment on governance, risk management, and control processes for the organisation. Assurance could be provided through Internal Audit, Management self-assessment, or any audit or review by an external party
Australian Standard for Compliance Programs (AS 3806-2006)	This standard provides principles and guidance for designing, developing, implementing, maintaining and improving a flexible, responsive, effective and measurable compliance program within an organisation.
Breach (Compliance Failure)	An act or omission whereby the University has not met its compliance obligations, processes or behavioural obligations.
Business Compliance Requirements	Compliance obligations that are considered desirable but that are not legislated or regulated. These might include internal policies and procedures, industry codes and standards, and some quality management certifications.
Changes to requirements (Significant)	Changes to compliance requirements that are likely to have a major impact on the organisation's processes. For example, the introduction of new laws, regulations or, changes to or the introduction of new obligations in existing requirements, that would cause a fundamental change in an operating process.
Changes to requirements (Minor)	Alterations to existing compliance requirements that will have a minimal impact on the organisation's processes. For example; small changes to the wording of obligations that have little or no impact on operating processes, or amendments to few minor obligations within a requirement that have little impact on processes.
Compliance	Adhering to the obligations of laws, industry and organisational standards and codes, principles of good governance and accepted community and ethical standards.1
Compliance Management	A series of activities that when combined are intended to achieve compliance.
Compliance Management Framework	The policies, processes, tools, templates, registers, and systems that define and support compliance management activities.
Compliance Policy	Articulates roles and responsibilities for managing compliance, and the related obligations for compliance management within the organisation.

Term	Definition
Compliance Requirement	A law (legislated or common law), regulation, government directive, standard, contract or internal policy/procedure that has been adopted by the organisation.
Compliance Risk Universe	Categories and sub-categories of compliance risks as defined by the organisation.
Control	A system, process, structure, or other activity that either reduces the likelihood or the consequence of a risk incident.
GRC	Governance, Risk Management, Compliance An integrated approach used by corporations to act in accordance with the guidelines set for each category. Governance, risk management and compliance (GRC) is not a single activity, but rather a firm-wide approach to achieving high standards in all three overlapping categories. (http://www.investopedia.com/terms)
Insignificant Breach	A breach rated as 'Low' or 'Very Low' when assessed using the Breach Assessment Criteria
Regulatory Compliance Requirements	Legislation, Regulation, Government Directives, Contract or Standards linked to Government Directives, Licences, Permits or Accreditations.
Material Breach	A breach rated as 'Medium', 'High' or 'Very High' when assessed using the Breach Assessment Criteria
Obligation	Specific actions that the organisation must undertake in order to comply with the corresponding compliance requirement.
Primary Owner (of a requirement)	The Business Unit with organisational responsibility for a compliance requirement (refer Secondary Owner definition).
Secondary Owner (of a requirement)	Primary responsibility for a compliance requirement lies with another owner/business unit, but where this business unit is responsible for compliance with certain obligations that correspond to this requirement.

Attachment B – Compliance Requirements Register EXAMPLE

Legislation	Jurisdiction
A New Tax System (Australian Business Number) Act 1999	Commonwealth
A New Tax System (Family Assistance) (Administration) Act 1999	Commonwealth
A New Tax System (Goods & Services Tax) Act 1999	Commonwealth
A New tax System (Goods & Services Tax Administration) Act 1999	Commonwealth
A New Tax System (Luxury Car Tax) Act 1999	Commonwealth
Aboriginal and Torres Strait Islander Heritage Protection Act 1984	Commonwealth
Age Discrimination Act 2004	Commonwealth
Agricultural and Veterinary Chemicals (New South Wales) Act 1994	New South Wales
Agricultural and Veterinary Chemical Act 1994	Commonwealth
Agricultural and Veterinary Chemicals (Administration) Act 1992	Commonwealth
Agricultural and Veterinary Chemicals Code Act 1994	Commonwealth
Agricultural Livestock (Disease Control Funding) Act 1998	New South Wales
Agricultural Tenancies Act 1990	New South Wales
Anatomy Act 1977	New South Wales
Animal Diseases (Emergency Outbreaks) Act 1991	New South Wales
Animal Research Act 1985	New South Wales
Animals Act 1977	New South Wales
Annual Holidays Act 1944	New South Wales
Annual Reports (Statutory Bodies) Act 1984	New South Wales
Anti-Discrimination Act 1977	New South Wales
Apprenticeship and Traineeship Act 2001	New South Wales
Archives Act 1983	Commonwealth
Associations Incorporation Act 2009	New South Wales
Australian Human Rights Commission Act 1986	Commonwealth
Australian Radiation Protection and Nuclear Safety Act 1998	Commonwealth
Australian Radiation Protection and Nuclear Safety (Consequential Amendments) Act 1998	Commonwealth
Australian Radiation Protection and Nuclear Safety (Licence Charges) Act 1998	Commonwealth
Australian Research Council Act 2001	Commonwealth
Australian Research Council (Consequential and Transitional Provisions) Act 2001	Commonwealth

Attachment C – Compliance Obligations Register

Legislation

Jurisdiction	**Government Authority / Administrative Body**
Subordinate Legislation	**Key Contact & Contact Details:**
Standards Codes	

General Information

Overview

Obligations

Liability

Management Framework

Executive Accountable

Compliance Coordinator

Operational Responsibility

Application

Risk Profile

Risk Rating	**Risk Likelihood**	**Risk Consequence**

Business units subject to obligation

Management Mechanisms

Policies

Procedures

Guidelines

Training

Activities

Reporting and Recordkeeping

Legislative Updates

How compliance is periodically reported

How compliance is recorded

How breaches are reported

More information

Attachment D - Annual Compliance Plan Template

This template, except for the end of year sign-off, will be completed annually, by the 15th of May, by school/directorate/unit managers to help document all relevant elements of their compliance program. School/directorate/unit managers will be asked to "certify" that they have complied with their plan on 30th April each year.

School/Directorate/Unit	
Accountable (name and position)	
Responsible (name and position)	
Consult (position / group)	
Inform (position / group)	

1. Compliance Responsibilities

Record the requirements where this school/directorate/unit has primary responsibility for management for the University. This table will be populated with information from the **Compliance Requirements Register.**

Requirement	Type of Requirement	Priority Rating	Manager Responsible
Note: add rows as required			

2. Reporting Requirements

Record reports, returns, statements or disclosures of compliance required to be filed by the school/directorate/unit during the year.

Requirement	Nature of Reporting	Due Date
Note: add rows as required		

3. Audit and Assurance Requirements

Record audit and assurance activities, both internal and external, planned to monitor compliance activities in the school/directorate/unit.

Requirement	Nature of Audit/Assurance	Due Date
Note: add rows as required		

4. Training Requirements

Record compliance training sessions, internal and external, to be undertaken by school/directorate/unit management and staff during the year.

Requirement	Nature of Training	Due Date
Note: add rows as required		

5. Sign-off

Sign off is to be completed at the start and end of each year.

Start of Year I agree that these are the compliance requirements relating to my school/directorate/unit and that I will manage them and will report all potential breaches in accordance with the breach reporting process.

Signature: ____

Print Name: ____

Title: ____

Date: ____

Reviewed and
Approved by: ________________________________Date:_______________
(Senior Executive)

Date sent to Vice-Chancellor via
the Audit and Risk Directorate: _______________________________________

End of Year I confirm that all the compliance requirements and obligations of this school/directorate/unit were managed in accordance with the Compliance Management Policy, all breaches and potential breaches have been reported in line with the breach reporting process and all training, assurance and reporting requirements have been completed.

Signature: ____

Print Name: ____

Title: ____

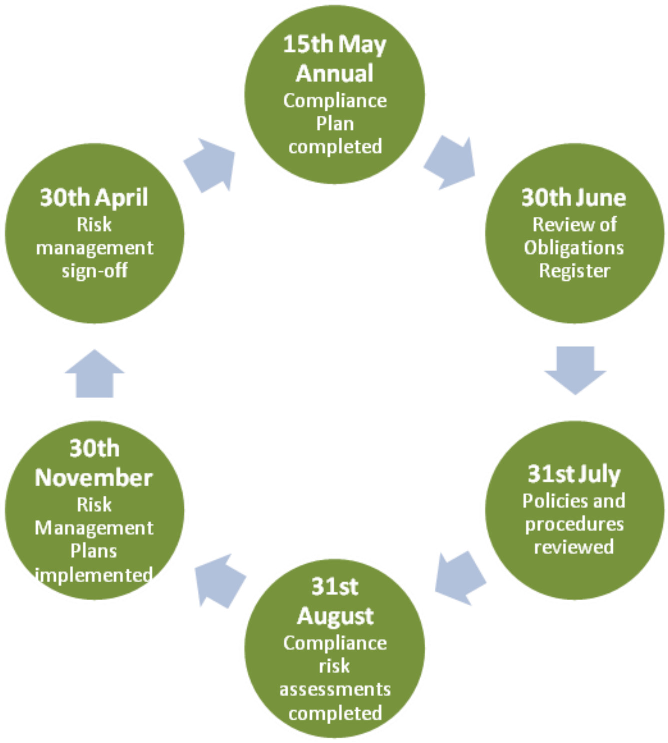
Date: ____

Reviewed and
Approved by: ________________________________Date:_______________
(Senior Executive)

Date sent to Vice-Chancellor via
the Audit and Risk Directorate: _______________________________________

Attachment E - Annual Compliance Management Calender

This document is used by Managers to document and diarise all their annual activities associated with their areas of compliance responsibility. These include completion of compliance plans, reviews of requirements and obligations, policy and procedure updates, risk assessments, reporting, training and assurance activities.


15th May Annual Compliance Plan completed
30th June Review of Obligations Register
31st July Policies and procedures reviewed
31st August Compliance risk assessments completed
30th November Risk Management Plans implemented
30th April Risk management sign-off

Month	Activity	Requirement	Responsibility
May	Complete Annual Compliance Plan	Compliance Policy	
June	Review and update Compliance Obligations Register for changes in legislation/regulations	Compliance Policy	
July	Update all policies and procedures to reflect changes in obligations	Compliance Policy	
August	Complete Compliance Risk Assessment	Compliance Policy	
September			
October			
November	Implement compliance risk management plans		
December			
January			
February			
March			
April	Self-assessment on operation of controls managing compliance risks	Compliance Policy	

Other Directorate/Unit/School specific activities (taken from the Annual Compliance Plan) to be incorporated into the Compliance Management Calender include:

- External reporting requirements
- External audit/assurance requirement
- Training requirements

Attachment F – Communications Plan Template

The use of this template is not required but schools/directorates/units may want to use this as a starting point for developing their communication plans.

Compliance Obligation or Requirement	Information to Communicate	Stakeholder	Communication Method	Frequency / Timing	Responsible Person	Expected Stakeholder Reaction / Involvement

Attachment G – Potential Breach Reporting Form

School/Directorate/ Unit:		**Breach Reported Completed by:**	
Identified by:		**Date identified:**	

PART 1

Summary of Potential Compliance Breach:			
Type of Potential Compliance Breach: (tick appropriate)			
Legislation:		Industry Standard/ Guideline:	
Internal Policy / Procedure		Material Contract:	
Licence / Permit Obligations:		Directive:	
Other: (Describe)			
Assessment of Potential Breach **(Very Low, Low, Medium, High or Very High)**			
Justification of Assessment **(describe the rationale behind the assessment rating)**			
Breach Investigation Team Members			
Breach Investigation Response Time			
Assessment signed-off by Executive Management			

PART 2

Investigation of Breach	
Internal consultation: (Describe results of internal investigation and consultation)	
Legal or other external consultation: (Describe interaction with lawyers or other external advisors and the advice received)	
Conclusion: (was the breach confirmed?)	
Final Rating of Breach:	
Resolution Steps at Date of Initial Assessment (including ongoing process improvements)	
Already Implemented	Still to be Implemented
Executive Review and Approval	
Breach Closed by: (include breach register update) **Date Closed:**	
Reviewed/Approved by Vice-Chancellor: **Date Reviewed:**	

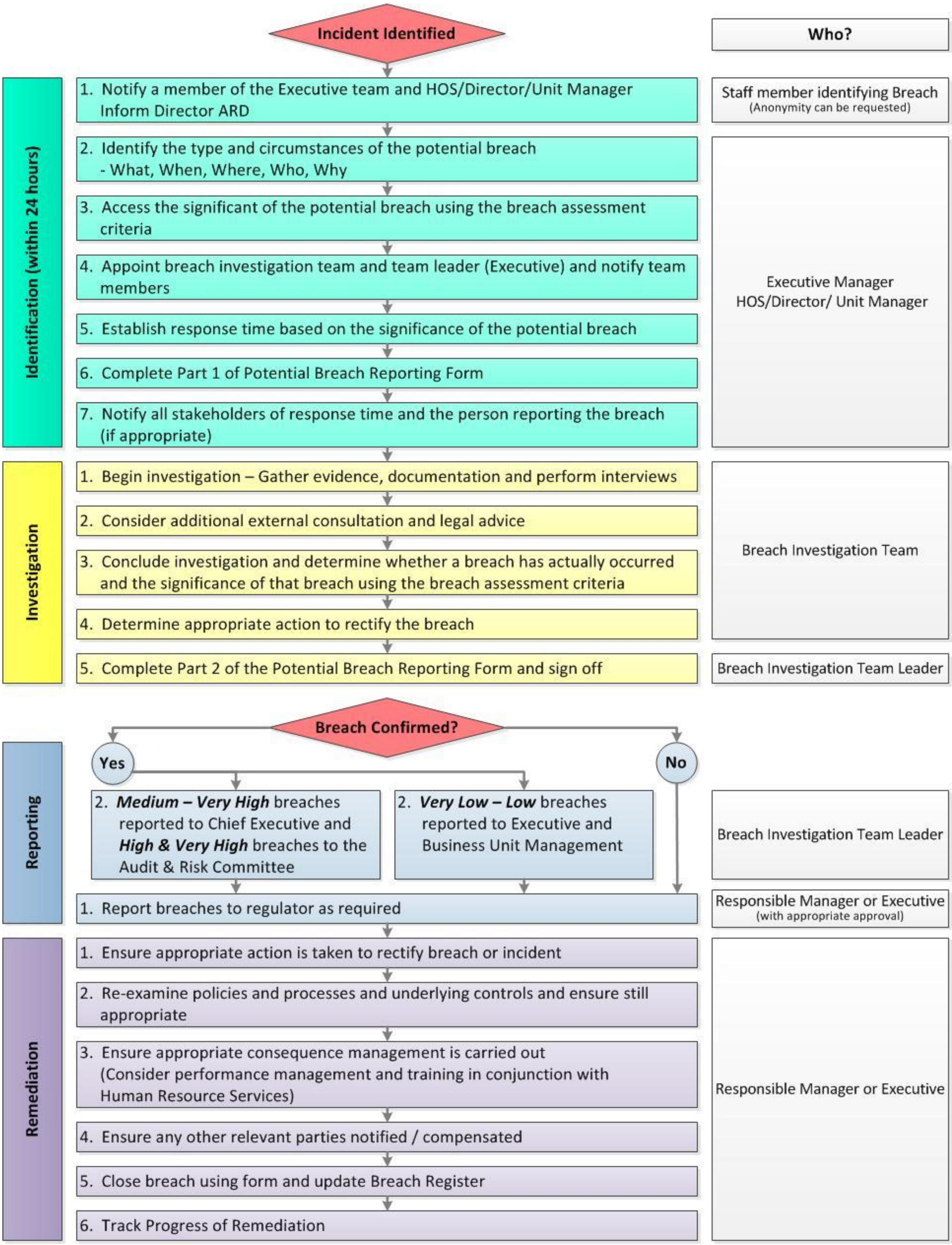
Reporting to Regulators		
Date Reported:	**By Whom:**	**Comments:**

Attachment H – Breach Register Template

The Director ARD will own the breach register and will use the potential breach register template to source information about the breach. This register is to be used for **confirmed breaches** only.

Date Breach Discovered	Date(s) of Breach	Description of Breach	Responsible Person	How was the breach identified?	Process & Responsibilities for Handling Breach	Date Breach Rectified and Closed

Attachment I – Breach Reporting Process



Incident Identified

Who?

Identification (within 24 hours)

1. Notify a member of the Executive team and HOS/Director/Unit Manager Inform Director ARD

Staff member identifying Breach
(Anonymity can be requested)

2. Identify the type and circumstances of the potential breach
   - What, When, Where, Who, Why
3. Access the significant of the potential breach using the breach assessment criteria
4. Appoint breach investigation team and team leader (Executive) and notify team members
5. Establish response time based on the significance of the potential breach
6. Complete Part 1 of Potential Breach Reporting Form
7. Notify all stakeholders of response time and the person reporting the breach (if appropriate)

Executive Manager
HOS/Director/ Unit Manager

Investigation

1. Begin investigation – Gather evidence, documentation and perform interviews
2. Consider additional external consultation and legal advice
3. Conclude investigation and determine whether a breach has actually occurred and the significance of that breach using the breach assessment criteria
4. Determine appropriate action to rectify the breach

Breach Investigation Team

5. Complete Part 2 of the Potential Breach Reporting Form and sign off

Breach Investigation Team Leader

Breach Confirmed?

Yes

No

Reporting

2. ***Medium – Very High*** breaches reported to Chief Executive and ***High & Very High*** breaches to the Audit & Risk Committee

2. ***Very Low – Low*** breaches reported to Executive and Business Unit Management

Breach Investigation Team Leader

1. Report breaches to regulator as required

Responsible Manager or Executive
(with appropriate approval)

Remediation

1. Ensure appropriate action is taken to rectify breach or incident
2. Re-examine policies and processes and underlying controls and ensure still appropriate
3. Ensure appropriate consequence management is carried out (Consider performance management and training in conjunction with Human Resource Services)
4. Ensure any other relevant parties notified / compensated
5. Close breach using form and update Breach Register
6. Track Progress of Remediation

Responsible Manager or Executive

Attachment J – Criteria or indicators of compliance breaches (in line with risk analysis criteria)

Note: As the nature of every potential breach will vary, the criteria below are for guidance only in determining the appropriate level of breach escalation. Each potential breach or indicator should be assessed on a case by case basis and reported as considered appropriate by the responsible Manager. If assistance is required, please contact the Director ARD.

	Potential Significant Breach			Potential Insignificant Breach	
Indicators ↓	**Very High**	**High**	**Medium**	**Low**	**Very Low**
Financial					
Costs – includes damages, fines, penalties, legal costs, loss of management time	>75% of UNE's budget surplus	>40% of UNE's budget surplus	>10% of UNE's budget surplus	>5% of UNE's budget surplus	<5% of UNE's budget surplus
Reputational					
Local, State, National or international adverse or unwanted publicity or media attention	Concentrated local or national media interest	Major story in national and/or local media	Significant item in local media	Low level mention and interest in local media	No media interest
Allegations of wrong doing, complaints from stakeholders or whistleblowing reports	Whistleblowing report upheld by Ombudsman. Student or stakeholder complaints upheld by authorities.	Whistleblowing report investigated by Ombudsman. Student or stakeholder complaints to authorities.	Whistleblowing report received. Repeated student or stakeholder complaints	Low level customer or stakeholder complaints	Isolated student or stakeholder complaints
Inquiry from ICAC, TEQSA Commissioner or other Government body	Severe relationship difficulties with Government body/bodies. Courses not accredited.	UNE embarrassment and/or inquiry. Restrictions on courses.	Issue with potential to affect course delivery/accreditation	Key questions by ICAC, TEQSA Commissioner or other external party	Some questions by ICAC, TEQSA Commissioner or other external party

	Potential Significant Breach			Potential Insignificant Breach	
Indicators ↓	**Very High**	**High**	**Medium**	**Low**	**Very Low**
People and Safety					
Death, injury or disability	Single death or injuries that include lifetime disabilities.	Injury involving long-term hospitalisation and significant rehabilitation.	Injury involving hospitalisation and/or rehabilitation.	Injury involving medical treatment other than first aid, and lost time from employment.	No injury or injury involving first aid, and no lost time from employment.
Industrial action or Union activity	Significant industrial relations disruption or union activity.	Industrial relations disruption and union activity.	Some industrial relations disruption or union activity.		
Loss of staff morale	Significant loss of key people.	Very high staff turnover.	Low staff morale and/or high staff turnover.	Recurring staff morale issues.	Isolated staff morale issues.
Legal and Compliance					
Criminal prosecution of the University, Executive or individual staff; or result in potential liability of an Executive	Civil claims or criminal prosecution.	Litigation. Licences or permits revoked.	Threats to licences or permits.		
Student/Customer Service Interruption					
Systematic errors / problems, loss of a student/customer service	Loss of a major service for > 5 days.	Loss of a major service for < 5 days.	Loss of a major service for < 1 day.	Loss of a minor service for < 5 days.	Loss of a minor service for < 1 day.
Operational Effectiveness					
Systematic errors / problems, loss of an internal service or management time	Loss of a major service for > 5 days.	Loss of a major service for < 5 days.	Loss of a major service for < 1 day.	Loss of a minor service for < 5 days.	Loss of a minor service for < 1 day.

	Potential Significant Breach			Potential Insignificant Breach	
Indicators ↓	**Very High**	**High**	**Medium**	**Low**	**Very Low**
Reporting Level					
Audit and Risk Committee	√	√	√		
Vice-Chancellor / CEO	√	√	√	√	
Executive Management and ARD Director	√	√	√	√	√

Attachment K – Complaints Register

Date	Received by	Complainant	Details of Complaint	Indication of Compliance Breach?	Forwarded to	Date	Details of Action Taken	Sign-Off