Griffith UNIVERSITY
Queensland, Australia

Procedure

Legislative Compliance Procedure

1.0 Purpose

These procedures describe the Compliance Management Program which:

- details how the objectives and principles of the Griffith University Legislative Compliance Policy will be achieved, and
- describes how the University will manage its compliance obligations through a risk-based approach integrated with the Enterprise Risk Management Framework.

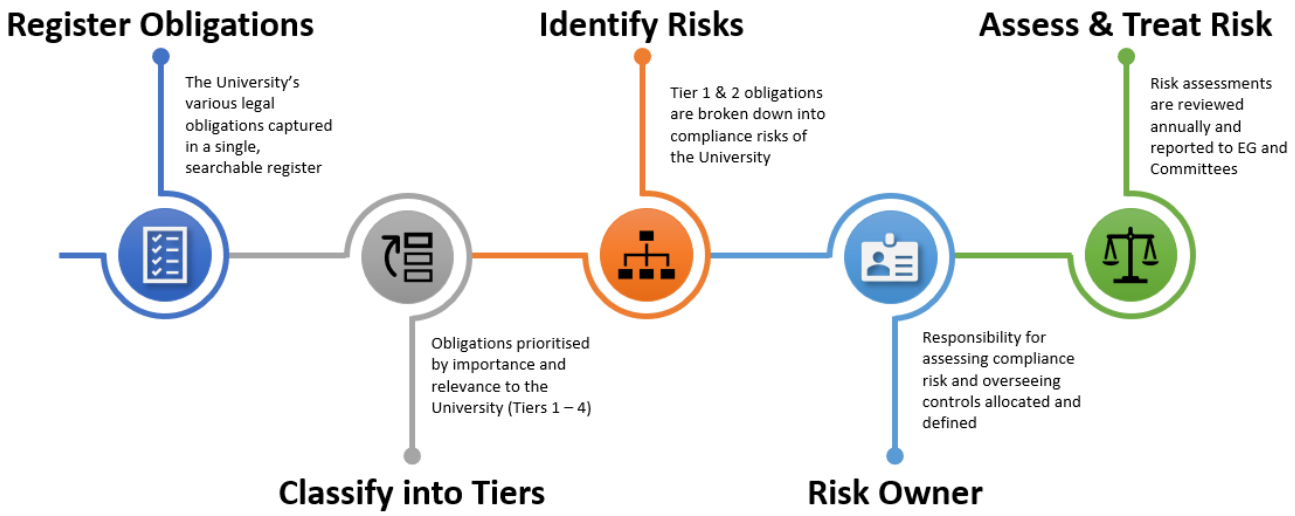
2.0 Scope

This procedure applies to all areas of the University's operations, including its staff, appointees of the University, its controlled entities, and to all activities authorised and conducted by or on behalf of the University.

3.0 Procedure

The diagram below shows how the Compliance Management Program employs a Prevent, Detect and Respond model, how ethical culture underpins all action, and provides a guide to navigate this document.

In brief, the key process is as follows:



3.1 3.1 Identify & Communicate Obligations

All identified legislative compliance obligations that are applicable to Griffith University must be captured in the Register of Compliance Obligations (ROCO). The ROCO will capture:

- The title of the Compliance Obligation (usually an Act, Regulation or associated Policy)
- The jurisdiction (usually Queensland or the Commonwealth).
- The objective/s of the legislative compliance obligation.
- A summary of the requirements within the compliance obligations relevant to the University.
- The regulator who is responsible for enforcing the compliance obligations.
- Where staff can find more information about the compliance obligations.
- The Tier that the compliance obligation is classified into.

The ROCO, as well as other relevant compliance documents and materials, will be made available to all staff through the Griffith University Compliance Intranet page.

Classification of Obligation by Tiers

As a higher education provider with diverse operations and fields of research, Griffith University has a large and complex body of legislation that it must comply with. The application and implications of legislative compliance obligations will vary significantly, for example:

- Applying to the University due to the nature of its legal entity, or due to the nature of its specific operations,
- Having widespread implications for all areas of the University, or only affecting a specific Element, or
- The consequences of breaching compliance obligations may be severe for the University, or may be relatively minor, depending on the circumstances of each breach and the legislation governing it.

Accordingly, legislative compliance obligations are classified into a set of Tiers as described by Table 1. The purpose of this classification is to prioritise and focus the assurance provided by the Compliance Management Program using a high-level assessment of the consequences of breaching an obligation.

Table 1 – Tier Classifications

TIER	CRITERIA
Tier 1	University-wide compliance obligation with potential for breaches to have Major or above consequences
Tier 2	Compliance obligations relevant to specific University Element/s with potential for breaches to have Major or above consequences.
Tier 3	University-wide obligation: • with potential for breaches to have Minor to Moderate consequences, or • that is relevant to the University and may need to be considered in identifying and assessing compliance risk.
Tier 4	Compliance obligations relevant to specific University Element/s: • with potential for breaches to have Minor to Moderate consequences, or • that is relevant to the University and may need to be considered in identifying and assessing compliance risk.

Note that:

University-wide means that the compliance obligation applies to the University because of its legal status and core functions, or because the University as an entity has committed to complying with a certain standard.

Relevant to specific University Elements means that the compliance obligation applies only because an Element/s within the University undertake certain operations and the compliance obligation would not otherwise apply. For example, owning and operating marine vessels to conduct scientific research attracting the application of marine safety laws to those operations.

Minor, Moderate and Major are references to the consequence descriptors used in Griffith's Enterprise Risk Management Framework.

The tiering classification of legislative compliance obligations is determined by the Compliance Function in consultation with key stakeholders and is approved by General Counsel.

Updating the Register of Compliance Obligations

Keeping the ROCO comprehensive, accurate and up to date is the responsibility of the Compliance Function. A number of measures will be employed to ensure that developments in the legislative environment are captured in the ROCO:

- Monitoring of updates through the LexisNexis Compliance Service and other legal update subscriptions,
- Scanning and monitoring of legal environment by Legal Services,
- Communication with regulators.

Where staff identify that a legislative compliance obligation is not captured in the ROCO, they should notify the Compliance Function. It is also expected that specialist staff should maintain an up-to-date understanding of legislation relevant to their professional duties, including by subscribing to relevant update services provided by regulators or other relevant bodies.

Griffith University may also incur additional Compliance Obligations through expanded operations or new fields of research. As part of good change management, the relevant manager is responsible for notifying the Compliance Function of the changes and any identified laws for inclusion in the ROCO.

New entries to the ROCO, and the tier classification, are approved by the General Counsel.

3.2 Identify Compliance Risk Owners

The appropriate assignment of responsibility is driven by how the compliance obligation/s affects University operations. Tier 1 and 2 compliance obligations will be analysed and broken down to identify how the University could breach the requirements of the obligation and to identify the Compliance Risk Owner.

The Compliance Risk Owner should be the staff member(s) who are best placed to:

- credibly assess the risk based on their position, responsibilities, and ability to monitor the operation of key internal controls, and
- take action to mitigate a compliance risk when it is not in line with the University's risk appetite.

The role does not imply ownership and responsibility for all compliance controls, as in many cases obligations will have cross-functional implications across the University. Often, the Compliance Risk Owner will need to engage broadly with stakeholders across the University, exercising enterprise leadership with the support of the Compliance Function, to ensure the effective mitigation of compliance risk.

The designation of Compliance Risk Owner must be approved by the relevant member of Executive Group. They are the key first line role for managing compliance risk.

3.3 Compliance Risk Assessment

All compliance obligations create the risk of a breach. A risk assessment approach enables the University to:

- Identify causal factors for a breach and relevant consequences,
- Identify the relevant areas that should be managing the risk of compliance breaches,
- Identify internal control measures needed to prevent, detect and correct breaches,
- Assess the level of risk and prioritise areas for focus and investment of University's resources,
- Integrate with the University's Enterprise Risk Management Framework and systems and templates used to assess risk and put into practice the University's risk appetite,
- Align with best practice – the Compliance Management Standard ISO37301.

The Compliance Risk Owner is responsible for conducting and documenting a risk assessment consistent with the Enterprise Risk Management Framework:

- The documented risk assessment will be stored in accordance with the risk management framework and be available for monitoring by the Compliance Function and reporting to management and the Audit Committee.
- The risk assessment should identify the key internal controls that are relied on to prevent, detect and correct compliance breaches, as well as the relevant area responsible for the internal control.

- The risk assessment should be maintained and updated for changes and events in the external and internal environment, including changes in staffing or structures, new or amended legislation and relevant incidents, as well as being formally reviewed at least annually.

A risk assessment is *required* for all compliance risks identified with Tier 1 and Tier 2 legislation. A risk assessment is *encouraged* for risks within Tier 3 & 4.

To be clear, compliance with obligations is mandatory, regardless of which Tier the obligation is classified into.

The role of the Compliance Function is to provide a second line of compliance risk management; to constructively question and challenge the risk assessments conducted by Compliance Risk Owners, and to provide advice and support about the compliance obligations and the application of the Enterprise Risk Management Framework and these procedures. The Compliance Function cannot override the assessment made by the Compliance Risk Owner or be delegated the responsibilities of the Compliance Risk Owner.

3.4 Annual Sign-off - Tier 1 & 2 Compliance Risks

The Compliance Function will develop an annual plan to review a set of Tier 1 & 2 compliance risks to provide assurance to management and the Audit Committee that compliance risks are being adequately managed in line with the University's risk appetite. The Compliance Risk Owner will be responsible for reviewing and updating the risk assessment in consultation with relevant stakeholder. As part of the annual review Compliance Risk Owner will need to confirm in writing:

- That internal controls are adequate and operating effectively, taking into account any new or amended requirements,
- That the risk rating has been assessed applying the Enterprise Risk Management Framework and is credible and reliable,
- All breaches relating to the legislative compliance risk have been reported in accordance with these procedures,
- Where a risk rating is not in line with the University's risk appetite, that a treatment action plan is in place to bring the risk to an acceptable position, or a risk acceptance is approved (see s.3.8).

The reviewed compliance risk assessment, and the written confirmation of the above, must be provided to the Compliance Risk Owners' Executive Group member for review and endorsement. This provides the Executive Group member the opportunity to exercise appropriate oversight and due diligence in relation to key legislative compliance risks managed within their group.

Following endorsement by the Executive Group member the Compliance Risks reviewed will be summarised into an Annual Compliance Report for the Audit Committee.

3.5 Documentation and Record Keeping

Regardless of what tier classification a compliance obligation falls in, internal controls for compliance should be documented and auditable, enabling the University to:

- communicate required processes, practices, or actions to relevant parties,
- demonstrate how it responds to compliance requirements, and
- enable the adequacy of that response to be reviewed and tested (e.g. by an incoming manager or internal audit).

The documentation should be appropriate to the specific operating environment that the obligation applies to. It does not need to be a formal policy or procedure and may take the form of, for example: local manuals or

protocols, training materials, contractual clauses, process maps, meeting agendas, papers or minutes, and workplace communication materials such as posters or reports.

Good recordkeeping practices – important for all University activities – takes on added importance when conducting activities regulated by legislation. In addition to general obligations under the *Public Records Act 2002* (Qld), legislation commonly creates specific record keeping requirements including penalties for non-compliance. See the Information Management Policy for more detail.

3.6 Reporting of Legislative Compliance Breaches

All staff should report suspected, actual or potential breaches to the staff's line manager in first instance, to be escalated to the respective Head of Element. The Head of Element is responsible for investigating and when a breach or near miss is established (in consultation with Legal Services, as required), reporting the matter using the Compliance Breach Reporting Form which will be available through the Griffith University Compliance Intranet page.

Breaches which fall within Table 2 below must be reported through to the Compliance Function and General Counsel as head of that function. The purpose is to ensure that the General Counsel is aware of any breach of legislation and is able to ensure that appropriate remediation action is being taken by the University.

Table 2 – Scope of Breach Reporting under this Procedure

IN SCOPE	OUT OF SCOPE
• Breaches of legislative compliance obligations by the University, regardless of the Tier • Near miss incidents, where a breach would have occurred but for a fortunate set of circumstances, indicating a weakness in compliance controls.	• Breaches of internal policies and procedures by staff or students, unless the breach also amounts to a breach of law.

Reports should be made promptly, ensuring that the appropriate University officers are aware and so that actions can be put in plan to prevent the breach or lessen the consequence of the breach.

Volunteers, visitors, guests, students, subcontractors are encouraged to report breaches through the YourCall hotline.

A central register of compliance breaches will be maintained by the Compliance Function detailing:

- the relevant compliance obligation
- the date the breach or near miss was identified
- a description of the circumstances
- a consequence rating based on the Enterprise Risk Management Framework
- action taken to mitigate
- the status of the breach (open or closed)

The register of compliance breaches will be used to report to senior management and the Audit Committee about any serious breaches and actions taken to respond. The register will be a confidential document managed within the Compliance Function.

3.7 Monitoring Regulatory Correspondence

Good compliance risk management involves having a clear and appropriate process for interacting with Griffith's key regulators with matters raised in correspondence communicated to appropriate parties within Griffith. Correspondence with regulators will also often alert the University to trends, issues, incidents or areas of focus relevant to managing compliance risk. To ensure there is transparency to regulator correspondence and enable the Compliance Function to detect new, emerging or changing compliance risks through this key information source - and able to act on it – a set of key regulators is identified and approved by the General Counsel. The register details:

- The regulator and the legislation they administer,
- Who is Griffith University's primary point of contact/s for liaising with the regulators about compliance matters and whether that person is nominated with the regulators as the contact point,
- Examples of the types of compliance correspondence made, and
- The process for storing correspondence and how this is monitored as a source of risk information. This will be achieved through establishing Key Risk Indicators that will be reported to and monitored by the Compliance Function.

Records of regulator correspondence relating to compliance matters will need to be accessible and monitored by the Compliance Function. This will include, for example:

- Notification of incidents to regulators (eg. material change notifications, workplace incidents)
- Regulator notices about taking, planning or considering enforcement action against Griffith University,
- Regulator notices invoking investigation powers in relation to a matter, or alerting Griffith University to a compliance matter affecting the higher education sector
- Reports by the regulator sent to Griffith University about compliance assessments undertaken.

The Compliance Function will report to Executive Group and Audit Committee about the level and nature of correspondence received to provide assurance that risk is being actively monitored.

3.8 Risk and Issue Treatment

When a risk assessment identifies that the risk of a breach is not consistent with the Universities risk appetite statement, then the Compliance Risk Owner must document a risk treatment plan, detailing responsibilities and timeframes, for mitigating the compliance risk. This treatment plan must be recorded with the risk assessment and be able to be tracked and monitored by the Compliance Function.

Alternatively, and only in exceptional circumstances where it is impractical to reduce the risk, a 'risk acceptance' can be sought. A risk acceptance is an informed, documented decision to take no further action to modify the level of risk. It should be considered a temporary position, to be reviewed at intervals to account for changed circumstances. As an exceptional position, it must be approved by senior management and reported to an appropriate University Committee. Relevant levels of approval for risk acceptance are defined in the Enterprise Risk Management Framework.

When a compliance breach is identified, through a risk assessment or otherwise, it represents an issue that needs to be rectified by:

- Following the reporting procedure at 3.6, and
- The Compliance Risk Owner, or other responsible staff member, developing an appropriate and robust treatment action/s including responsibilities and timeframes. The treatment action will be recorded in the compliance breach register and will be monitored and followed up by the Compliance Function.

The Compliance Function will ensure remediation action is appropriate, followed through, and for Tier 1 & 2 compliance obligations, that the risk assessment is updated as appropriate.

3.9 Executive, Committee & Council Compliance Reporting

An Annual Compliance Report will be prepared for the Executive Group and the Audit Committee. The objective of the report is to inform the Committee about the status of the University's compliance risk profile and the operations of the Compliance Function. In addition, the Compliance Function will report on significant compliance breaches and action being taken to remediate. The Office of the General Counsel will also provide regular reporting on legal and compliance matters.

3.10 Continuous Improvement

The Compliance Function will review information gathered through risk assessment and use insights from the risk profile to develop a Compliance Improvement Plan which will outline the key initiatives for addressing high risk compliance areas. This may include detailed and targeted second line risk reviews, control improvement support and the development of training and communication material, depending on the risk-based priorities of the University.

3.11 Review of Compliance Program

The Compliance Program and these procedures will be subject to continual improvement and formal review every 3 years. This management review should be conducted with the assistance of an operationally independent, appropriately trained and competent person/s, and address the appropriateness, effectiveness and adequacy of the Compliance Management Program.

3.12 Summary of Requirements

The table below identifies the requirements for compliance risk management at the first line across the Tiers.

Table 3 – Summary of First Line Compliance Program Requirements by Tier

	Risk Assessment (See 3.3)	Annual Review of Risk (See 3.4)	Documentation and Record Keeping (See 3.5)	Breach Reporting (See 3.6)
TIER 1	Required	Required	Required	Required
TIER 2	Required	Required	Required	Required
TIER 3	Encouraged	No	Required	Required
TIER 4	Encouraged	No	Required	Required

4.0 Roles & Responsibilities

ROLE	RESPONSIBILITY
Vice Chancellor and Executive Management	Promote the Compliance Program and a positive compliance culture across the University. Be aware of, and exercise, legislative duties as executive officers with responsibility to take reasonable steps to ensure compliance by the University. Ensure Compliance Risk Owners have the appropriate resources to effectively manage compliance risk, consistent with the University's Risk Appetite. Challenge and question risk assessments to ensure that assessments are robust, comprehensive and appropriate stakeholders have been engaged.
Chief Operating Officer	Accountable for the Legislative Compliance Policy and the implementation of the Compliance Management Program.
General Counsel	Responsible for the development and implementation of the Compliance Management Program. Head of the Compliance function.
Compliance Risk Owners	Conduct and keep up to date a documented risk assessment. This includes reviewing the risk assessment when there are changes in the underpinning legislation, or in response to relevant changes in the University, or when relevant incidents are detected. Ensure the implementation and maintenance of adequate, effective and economical internal controls for meeting relevant compliance obligations.

	Conduct an annual review of compliance risk assessments. Ensure that any treatment actions to mitigate unacceptable compliance risks are appropriate, documented, tracked and effectively resources. Take reasonable steps to document your process for managing compliance within your area and ensuring an appropriate handover process is undertaken if the person undertaking the Compliance Risk Owner's function changes, including notifying the relevant Executive Group member of the handover.
Compliance Control Owner	Responsible for designing, implementing and monitoring the effectiveness of a control. This includes informing the risk owner about the status of the control.
Compliance Manager	Act as an advisor to Compliance Risk Owners and provide decentralised compliance risk management leadership. Maintain the Register of Compliance Obligations, in consultation with relevant stakeholders. Monitor and review compliance risk assessments and treatment actions. Facilitate the annual review of Tier 1 and 2 compliance risks. Report to senior management and the Audit Committee on compliance risks and breaches. Maintain the Compliance Breach Register and educate and advise on corrective action, secure commitment for action plans and follow up to ensure accountability. Proactively address and resolve enterprise-wide compliance areas of concern, strengthen compliance processes/controls and generally promote the objectives of the Compliance Program, including by identifying and participating, as appropriate, on University working groups and compliance governing committees Assist Internal Audit in developing an annual audit plan to provide assurance about key areas of compliance vulnerability and risk. Develop and deliver training and communication materials about compliance obligations.
All Staff	Comply with compliance obligations relevant to their position and duties. Accept and value the duty to uphold the law as part of an ethical principle of working for a statutory body in Queensland. Report compliance breaches in accordance with Procedures. Comply with the Code of Conduct and your employment agreement. Participate in risk assessments when required. Maintain knowledge and understanding of compliance obligations relevant to a staff member's professional duties at the University.

5.0 Definitions

Compliance Obligations are a law, or other instrument/document made binding on Griffith University by a law, that regulates the University and its operations.

Compliance Risk is the likelihood of an event that is a breach of a compliance obligation/s and the consequences of that event for achieving the objectives of Griffith University.

Compliance Control means a measure taken by the University with the purpose or effect of mitigating a compliance risk.

Compliance Breach means an event where Griffith University has demonstrably failed to achieve the requirements of a compliance obligation.

Compliance Function means the staff within the Office of the General Counsel with designated responsibility and authority for the operation of the Compliance Management System. The role of the function is to assist senior management in effectively managing compliance risks.

Internal Controls means measures taken to mitigate the risk that, in the context of this procedure, compliance obligations are not breached, or to detect and remediate a breach when it occurs. For example, it includes policies, procedures, training programs, delegations and approval processes, reporting, and inspections. Note: audits are not properly considered controls, rather they operate to provide assurance about internal controls.

Auditable means that an internal control can be audited; able to be examined by an independent party to ascertain what the internal control aims to achieve, how that objective is to be achieved, and form an opinion as to whether the internal control is operating effectively to achieve its purpose.

First, Second and Third Lines refers to the different roles in the 3 Lines Risk Management Model:

- 1st Line – owns and is accountable for identifying and managing risk and issues.
- 2nd Line – reviews and effectively challenges the management of risk with independent oversight over risk profiles and responsibility to appropriately escalate issues when required. In this context is the Compliance Function.
- 3rd Line – provides independent assurance that frameworks for managing risk are adequate, have been implemented, and are operating effectively. In this context this is the Internal Audit team as well as any external assurance activity conducted by regulators.

The Enterprise Risk Management Framework includes a diagram outlining the 3 Lines Risk Management Model at Griffith University.

Adequate and Operating Effectively means that an internal control:

- Is designed to address the risk/s that it is intended to mitigate,
- Is implemented as designed with appropriate communication, training and documentation,
- Has evidence that can demonstrate the operation of the control.

Compliance Risk Profile means the collection of data, metrics and information that provides an enterprise view of the organisation's exposure to compliance risk; for example identifying areas of Low, Medium and High risk.

INFORMATION

Printable version (PDF) Downloadable version (Word)

Title	Legislative Compliance Procedure
Document number	2023/0001191
Purpose	These procedures describe the Compliance Management Program, detailing how the objectives and principles of the Griffith University Compliance Policy will be achieved.
Audience	Staff
Category	Governance
Subcategory	Risk and Integrity
Approval date Effective date	8/12/2022 8/12/2022
Review date	2025
Policy advisor	Compliance Manager
Approving authority	General Counsel

RELATED POLICY DOCUMENTS AND SUPPORTING DOCUMENTS

Legislation	N/A
Policy	Legislative Compliance Policy Enterprise Risk Management Policy Code of Conduct Public Interest Disclosure Policy Information Management Policy
Procedures	Enterprise Risk Management Framework
Local protocols	N/A
Forms	Register of Compliance Obligations Register of Compliance Breaches Annual Sign-off template Compliance breach reporting form