

Compliance Management Framework

Approving authority	University Council
Approval date	6 August 2018 (3/2018 meeting)
Advisor	Vice President (Corporate Services) vpcorporateservices@griffith.edu.au (07) 373 57343
Next scheduled review	2023
Document URL	http://policies.griffith.edu.au/pdf/Compliance Management Framework.pdf
TRIM document	2018/0000050
Description	This framework sets out the University's approach for the management of its compliance obligations and risks. The framework is a risk-based approach to compliance management

Related documents

[Code of Conduct](#)

[Public Interest Disclosure Policy](#)

[Register of Compliance Obligations](#)

[Risk Management Policy](#)

[Risk Management Framework](#)

[\[Commitment to Compliance\]](#) | [\[Responsibilities for Compliance\]](#) | [\[Compliance Program\]](#) | [\[Incidents of Non-Compliance\]](#)

1. COMMITMENT TO COMPLIANCE

As a public entity, the University has a responsibility to identify and comply with all relevant compliance obligations. The University should “...take these obligations into account when establishing, developing, implementing, evaluating, maintaining and improving its compliance management system. The compliance management system should reflect the organisation’s values, objectives, strategy and compliance risks”¹.

The University's commitment to compliance is demonstrated by:

- The sponsorship and support from University Council, Audit Committee and Finance, Resources and Risk Committee for the University's compliance program;
- The active engagement of Senior Management in the identification and management of compliance issues and risks;
- Leadership, at all levels to promote, encourage and support compliance;
- A compliance culture that identifies and manages compliance risks to ensure the achievement of the University's strategic objectives;
- A commitment to the management, monitoring and reporting of compliance issues and risks;
- Integration of compliance obligations into business processes and operations to drive effective and accountable decision making;
- Appropriate competencies and training to discharge compliance responsibilities and provide support for the management of compliance obligations;
- Appropriate monitoring and reporting mechanisms that will assist in identifying instances of non-compliance and tracking remedial actions; and

¹ Australian Standard AS/ISO 19600:2015 Compliance management systems - Guidelines

- The allocation of resources throughout the University to manage compliance obligations.
-

2. RESPONSIBILITIES FOR COMPLIANCE

2.1 All staff

In accordance with the University's Code of Conduct, and the principle of respect for the law, all University staff should be conscientious in seeking to comply with relevant obligations and shall take every reasonable measure to ensure compliance in the course of their duties. All staff are required to report incidents of non-compliance (refer to section 4. Incidents of Non-Compliance).

2.2 University Council

The Council is responsible for approving this Compliance Management Framework.

The Vice-President (Corporate Services) is responsible for ensuring that the University Council receives adequate reporting through the Audit Committee on compliance issues.

2.3 Audit Committee

The Audit Committee is responsible for:

- Reviewing with the Vice President (Corporate Services) and the Director Audit Risk and Compliance, the University's Compliance Monitoring Plan, including legal and regulatory requirements; and
- Ensuring that it receives an annual report and ad hoc reporting as required from the Vice President (Corporate Services), and that it identifies and requests follow-up action on any recommendation or incidents of non-compliance.

2.4 Finance, Resource and Risk Committee

The Finance, Resources and Risk Committee is responsible for advising the University Council on the University's risk management policy and strategy, and for monitoring the implementation of risk management strategies. The Finance, Resources and Risk Committee will review and endorse the Compliance Management Framework to Council for approval.

2.5 Vice Chancellor / Executive Management

The Vice Chancellor and the Executive Management are responsible for setting the tone and the culture for compliance across the University by supporting the compliance program.

2.6 Vice President (Corporate Services)

The Vice President (Corporate Services) is responsible for implementation of the compliance program, including:

- Ensuring processes are in place for maintaining the Register of Compliance Obligations;
- Preparing reports to University Council through the Audit Committee on compliance issues;
- Ensuring training programs are developed for relevant obligations to raise awareness of the University's obligations; and
- Providing advice to Compliance Owners and other staff on compliance obligations and issues.

2.7 Senior Managers

The management of compliance will chiefly occur within operational areas, and non-compliance will be dealt with through existing operational level management processes. However, compliance issues will on occasion necessitate an escalation to senior management because of the nature of the risk or resources involved. In these cases, it is the responsibility of senior managers to review the situation and implement remedial procedures.

At all times it is the responsibility of senior managers to remain aware of the compliance obligations allocated to operational areas under their supervision, and the designated Compliance Owner's management of these obligations.

2.8 Compliance Owners

Compliance Owners are designated for all obligations, as noted in the Register of Compliance Obligations, and are normally the head of the operational area allocated responsibility for ensuring compliance with a specific obligation. There may be multiple Compliance Owners for certain obligations.

A Compliance Owner is required to:

- confirm that they are seeking, in the course of their operational activities, to ensure compliance with each obligation for which they are the designated Compliance Owner;
- Ensure processes and procedures are in place to comply with compliance obligations (refer to section 3.1.1);
- Identify and communicate compliance risks in their area of responsibility to their relevant Executive Management, stakeholders and interested parties;
- Advise the Compliance Manager on compliance obligations identified to ensure the accuracy and currency of the Register of Compliance Obligations;
- Ensure staff who perform compliance activities are appropriately trained and report any issues or concerns relating to their compliance activities;
- Monitor and review compliance obligations and controls with sufficient frequency to ensure the currency and ongoing effectiveness of controls;
- Ensure the cost effectiveness of compliance is considered when assessing the adequacy of the compliance response;
- Seek assurance on the effective management of their compliance obligations through participation in the Compliance Monitoring Plan;
- Report to Executive Management, stakeholders and interested parties on any incidents of non-compliance and the remedial action taken to address them, including any ongoing non-compliance issues; and
- Facilitate any ad hoc reviews to meet Audit Committee and Finance, Resources and Risk Committee and any third party requirements.

Compliance Owners are expected to maintain a sound knowledge of their designated obligations, and should convey advice of new obligations or changes to existing ones to the Compliance Manager.

2.9 Compliance Manager

Through delegated responsibility from the Vice President (Corporate Services) and the Director, Audit Risk and Compliance, the Compliance Manager is responsible for:

- Ensuring the Compliance Management Framework is implemented, maintained and reviewed for effectiveness;
- Conduct periodic compliance risk assessments to identify potential high risk areas of compliance vulnerability and develop risk mitigation plans;
- Ensuring the Compliance Monitoring Plan is developed, implemented, maintained and reviewed for effectiveness;

- Maintaining the Register of Compliance Obligations;
- Identify, in conjunction with Compliance Owners, compliance requirements arising from an obligation; and
- Act as an advisor to Compliance Owners.

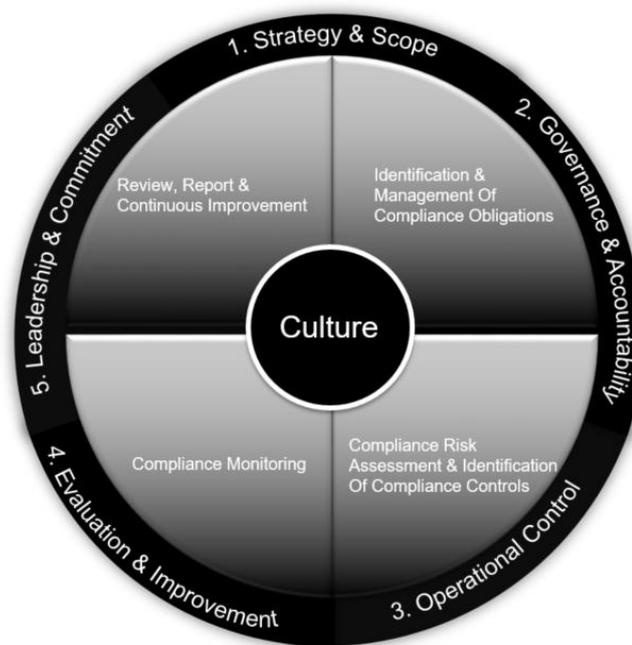
3. COMPLIANCE PROGRAM

The University's compliance program is an important element of the University's corporate governance framework.

The compliance program aims to prevent, and where necessary, identify and respond to, non-compliance with the University's obligations under laws, regulations, codes and its own organisational standards. An important priority for the compliance program is to encourage a culture of valuing compliance with obligations, consistent with the profile of a good corporate citizen.

The compliance program's general aims are pursued through the following key elements and illustrated below:

- **Identification** and **management** of the University's **compliance obligations** and allocation of responsibility to the relevant operational areas for ensuring compliance with obligations. A comprehensive list of the University's compliance obligation is kept in the Register of Compliance Obligations;
- **Compliance risk assessment** to identify high risk exposure areas and identify where management efforts are required to manage these compliances related risks through **identification of compliance controls**;
- **Compliance monitoring** will occur based on the results of the compliance risk assessment to assist relevant organisation areas to improve procedures and internal control for high-risk compliance areas and to provide assurance on how well the University meets its obligations, and where and how it could improve, including identification of any non-compliance and remedial action taken; and
- **Review** of compliance risks and **report** through the established governance channels and the promotion of **continuous improvement** through competency and training to staff and management on the importance of compliance with specific obligations, as well as commitment to compliance as an organisational value in line with the University's Code of Conduct.



3.1 IDENTIFICATION AND MANAGEMENT OF COMPLIANCE OBLIGATIONS

The University as a large and complex statutory authority, has a significant number of compliance obligations, at the State, Commonwealth and International level. To ensure that the University can comply with all its obligations, it is important to identify legislation and other legislative instruments which impose a compliance obligation. These obligations may arise because the University is, for example, an employer, a provider of goods and services, a statutory body or a recipient of Commonwealth funding. Compliance obligations might include:

- Reporting requirements (provision of statistics or information);
- Requirements for accreditation, registration or licensing;
- Complying with timeframes set down by the legislation for performing activities;
- A requirement to provide a specified service or range of services;
- Restrictions or limitations on how these services can be offered;
- Financial obligations;
- Professional industry standards; and
- Accepted ethical standards.

3.1.1 Management of Compliance Obligations

To ensure the University can demonstrate compliance with its obligations effectively and efficiently and the reasonable management thereof, the University will:

- Adopt an enterprise approach to the management of compliance to ensure its processes and procedures:
 - Explicitly address legal and regulatory obligations;
 - Are integrated into all organisational activities and practices to enable compliance management to be an integral part of management decision making, examples include:
 - Obtaining accreditation, registration or licensing;
 - Reporting to a relevant authority on statistics, or activities relating to compliance;
 - Developing a policy or procedure at either University or operational area level;
 - Employing or training staff to undertake compliance related-duties;
 - Creating a particular committee or working group to oversee compliance-related activities;
 - Maintaining records on activities undertaken by staff or student in accordance with the legislation;
 - Offering regular training programs for staff or the University community on the obligation; and
 - Developing a procedure for reporting non-compliance incidents within the organisational unit.
 - Are context driven and prioritised according to the assessed level of the University's risk exposure;
 - Are systematic, structured and consistent with University's Risk Management Framework;
 - Are documented to demonstrate evidence of compliance in order to protect and enhance the University's reputation; and

- Are dynamic, iterative and responsive to change and allow for continual improvement of the procedures and processes as and when required.
- Compliance obligations are appropriately grouped and assessed to identify the specific action required of the University to meet its obligations (Register of Compliance Obligations);
- Ensure clarity of roles, responsibilities and accountabilities to nominated staff for the effective management of obligations, including monitoring, reviews and assurance;

Compliance procedures are not “add-on” activities, and do not require additional resources. Compliance procedures should integrate with normal business activities of the relevant organisational unit.

3.2 COMPLIANCE RISK ASSESSMENT AND IDENTIFICATION OF COMPLIANCE CONTROLS

Breaches of laws, regulations, codes of conduct or the University’s own systems and processes is a compliance risk which can potentially have a significant impact on the University’s operations and impact the finance and or reputation of the University.

The Compliance Manager will undertake an annual compliance risk assessment in consultation with Compliance Owners, to identify the compliance risk exposures, including the likelihood of a risk occurring, the potential reasons for the occurrence and the potential severity of its impact so that compliance risks can be appropriately assessed and managed.

The University’s Risk Management Framework methodology will be adopted to identify, analyse, evaluate and effectively manage the compliance risks.

The compliance risk assessment will include using the Register of Compliance Obligations as the basis to identify compliance obligations and risks. This includes:

- Identifying the current operational control and the extent to which compliance requirements are being met;
- Identify high compliance risks and any deficiencies within the control processes;
- Monitoring of high compliance risks; and
- Provide timeframes for reporting and continuous improvement initiatives.

3.3 COMPLIANCE MONITORING

Under oversight and direction from the Audit Committee and the Finance Resources and Risk Committee, the following three lines of defence within the University will monitor and review compliance activities:

- **First Line of Defence:**

Compliance Owners are responsible for compliance with specific obligations with support from staff who perform function related compliance activities and are to participate in the Compliance Monitoring Plan.

- **Second Line of Defence:**

The Compliance Manager assists Compliance Owners with compliance obligations and provides assurance through the Compliance Monitoring Plan through a risk-led approach on high-risk compliance areas.

- **Third Line of Defence:**

Internal Audit, External Audit and independent assurance provider’s (i.e. regulatory bodies or certification bodies) provides independent assurance and oversight of the effectiveness of governance, risk management and internal monitoring and control functions.

3.3.1 Compliance Monitoring Plan

The University is committed to maintaining an effective Compliance Monitoring Plan that seamlessly integrates into its operational practices.

A Compliance Monitoring Plan will be developed from the compliance risk assessment and will capture high compliance risks and enable the systematic approach to the management of compliance obligations and risks for the university. In conjunction with other compliance activities undertaken throughout the University, the Compliance Monitoring Plan will provide further assurance that the University is compliant with its high-risk obligations.

Compliance monitoring is a preventative measure to confirm that controls are in place and operating effectively.

Based on the Compliance Monitoring Plan the Compliance Manager will work with Compliance Owners to ensure appropriate procedures including internal controls are in place to manage the compliance obligation and mitigate the risk of non-compliance.

3.4 REVIEW, REPORT AND CONTINUOUS IMPROVEMENT

3.4.1 Review and Report

Compliance Owners will maintain records of compliance to demonstrate evidence of actual compliance or non-compliance for review and reporting purposes.

The Compliance Manager will review and report upon the Compliance Monitoring Plan and will provide reports, as appropriate, to improve the University's compliance processes to the Compliance Owners, the Audit Committee and the Finance, Resources and Risk Committee. The report will capture high compliance risk issues and or compliance failures and areas of improvement. The compliance monitoring report will typically include:

- Any matter that the University is required to notify;
- Significant changes to compliance obligations, the impact to the University and the proposed course of action;
- Measure of compliance performance;
- Corrective action undertaken; and
- Evidence of the compliance program's effectiveness, achievements and trends.

3.4.2 Continuous Improvement

The Compliance Monitoring Plan is to be continuously reviewed and improved to enhance and promote the University's compliance culture.

Compliance Owners should ensure that procedures for managing compliance with obligations are regularly reviewed and improved as required. This provides assurance that the procedures in place remain relevant to, and adequate for, proper management of the obligation. Continuous improvement activities may include:

- A one-off or trial training program run by an organisational area;
- Establishment of advisory service for particular activities or commencement of a new obligation;
- Any audits undertaken on specific activities;
- Any policies, procedures or processes developed and/or documented and ensuring there are no duplication of compliance efforts;
- Establishment of any working parties or committees for specific issues;
- Any projects undertaken relating to compliance activities;

- Compliance process reviews and improvements;
 - Currency of compliance obligations captured within the Register of Compliance Obligations and the Compliance Monitoring Plan; and
 - Review of allocation of compliance responsibilities.
-

4. INCIDENTS OF NON-COMPLIANCE

Compliance Owners are to report on all non-compliance incidents and the management of the non-compliance to the Director Audit Risk and Compliance and the Compliance Manager as and when such incidents occur.

Information received from Compliance Owners during this process is used to advise the University Council through Audit Committee and the Finance Resources and Risk Committee of high-risk non-compliance incidents or significant compliance trends. Actions may be taken on the basis of this reporting by Executive Management to clarify any non-compliance incidents which have not been satisfactorily addressed by an organisational area.

A staff member who wishes to report any incident of non-compliance should approach the relevant designated Compliance Owner if the incident relates to a specific obligation, or alternatively, a staff member may follow the Public Interest Disclosure policy.