Compliance Framework

POLYTECHNIC
INSTITUTE AUSTRALIA

Compliance Framework

Contents

1. Compliance Management Framework

Polytechnic Institute Australia (the Institute) is a nimble organisation that requires a compliance management framework that supports the institute without creating additional "compliance burdens".

Compliance has important links to risk and given that the Institute's obligations with regards to the *Tertiary Education Quality and Standards Agency Act* 2011, the *Education Services for Overseas Students Act* 2000 and other legislation, the Institute requires a compliance management framework that allows it to demonstrate an appropriate standard of governance without over complicating the process.

1.1. Purpose of the Compliance Management Framework

The purpose of this document is to provide an overarching framework for the policies, procedures, structures and tools that are aimed at identifying and managing the Institute's compliance obligations.[1]

This Compliance Management Framework ('the Framework') aims to create an integrated, strategic and consistent approach to the management of the Institute's compliance obligations and articulates the process for identifying, recording, evaluating, prioritising and monitoring the Institute's compliance obligations. The Framework details a structure for responsibilities and accountabilities and specifies the broader compliance management approach that the Institute has adopted.

1.2. What is compliance?

For this Framework "compliance" is defined as "adhering to the requirements of laws, industry and organisational standards and codes, principles of good governance and accepted community and ethical standards" (*AS 3806-2006, Australian Standard: Compliance programs*). Compliance is central to good governance.

The Institute's compliance obligations refer to the laws, regulations, codes, policies, and procedures with which the Institute is required to comply.

1.3. The importance of compliance management

The Institute has a range of obligations with which it is required to comply. The Institute has accountability to both internal (e.g. Quality and Risk Committee) and external (e.g. TEQSA), bodies. The Institute needs to demonstrate it is fully aware of its compliance obligations and the associated risks and that it is meeting and managing these obligations consistently and appropriately.

Compliance management is important because compliance obligations and their associated risks are continually evolving — a strategic approach is required to facilitate the implementation of sound

[1] It should be acknowledged that this document is in the majority a copy of the similar material from Deakin University at Compliance Management Framework (deakin.edu.au)

practices aimed at keeping abreast of this evolution. Remaining well-informed regarding the Institute's compliance requirements and obligations, and ensuring that there are strategies in place to guide the Institute and its staff on matters of compliance, is a vital task and one that is critical to the success of the Institute.

1.4. Accountabilities and responsibilities

The Compliance Management Framework promotes a culture where compliance is valued and as such every Institute's staff member has an important role to perform in establishing and maintaining a robust compliance management culture and process.

Notable responsibilities include the Executive and the Board of Directors, who hold ultimate responsibility for compliance management and the Compliance, Quality and Risk Manager who is responsible for oversight, guidance and advice on the broader compliance management process. Key responsibilities are outlined in Appendix A: *Responsibility and Accountability for Risk and Compliance Management*.

1.5. Internal Audit Registers

Internal registers are used to record the Institute's compliance obligations and to ensure that the Institute can effectively and consistently manage the risks associated with non-compliance. The Compliance Obligations Register contains the results of the compliance management process, and it documents the identified compliance obligations, any associated compliance risks, and the method of evidence of compliance such as an internal or external audit, along with an assessment of the how the noncompliance is to be remediated and by whom. The Compliance Obligations Register and Internal Audit templates are stored in the Compliance Drive.

A delegated or responsible officer is determined for each compliance obligation, who has overall responsibility for managing compliance with obligations throughout the Institute. The most appropriate staff to hold these positions are determined by the Executive and/or senior management, in consultation with the Compliance, Quality and Risk Manager.

There are currently two Internal Audit templates: the HESF internal audit register and the CRICOS templates. Additional templates may be developed as required against different legislation as required.

The outcome(s) determined from reviewing the Compliance Obligations Register and completed internal audits are reported to the Quality and Risk Committee and any necessary remediation placed in a remediation plan.

Once the remediation has been completed that annual cycle of compliance review is completed.

1.6. Annual Compliance Schedule

Each year the Compliance, Quality and Risk Manager will set the compliance schedule to ensure that

compliance obligations are audited or attested to and that any potential risk exposures are managed.

2. Compliance Management Methodology

2.1. Compliance Management Methodology

The Risk and Compliance Management Policy and Procedure underpins the Compliance Management Framework.

There is a standardised approach to the Institute's management of compliance and this process is aligned and consistent with the AS3806-2006/ISO 37301:2021. The diagram below, based on material from Deakin University[2], shows the five main stages in the compliance management process and these elementsare described in further detail in the "Compliance Management Methodology" section of the Framework.

[2] Compliance Management Framework (deakin.edu.au)

Compliance Framework

Figure 1: The five main stages in the compliance management process

2.2. Identifying compliance obligations

The Institute has a wide range of compliance obligations including legislation, orders issued by regulators, judgements of courts or tribunals, and relevant industry codes and standards. The Institute is also required to comply with its own policies and procedures, as well as with any agreements and contracts it has with external parties.

With regards to legislative and regulatory compliance obligations, the Compliance, Quality and Risk Manager may take advice from the Institute's external legal sources or other reputable sources on any new/amended obligations affecting the Institute. This information is then distributed by the Compliance, Quality and Risk Manager to the affected Compliance Obligation Owning Committee and the Responsible Officer. The Responsible Officer who is responsible for the area will complete a Business Impact Report (using the provided template) to report the significance and scope of the obligation change.

In addition to an examination of Institute operations, compliance requirements and obligations are identified through:

- communication with legal, regulatory and industry bodies
- legislative updates
- professional associations and memberships
- internal communication (i.e. workshops)
- research and benchmarking with other institutions (i.e. better practice)

2.3. Compliance Risk Management

Risk Management is a set of components/elements that provide the foundations for designing, implementing, monitoring, reviewing, and continually improving risk minimisation within the Institute. This includes the creation of policy and procedures and establishing a framework and system for reviewing and monitoring risks.

Compliance obligations, when breached, pose risks to the Institute achieving its strategic objectives. Some of these risks will have the potential to have a major impact on the Institute and therefore may require more specialised attention. By expressing these risks as compliance risks, it allows the Institute to monitor the obligation more closely and to ensure that any negative impact is minimised.

All key compliance obligations are managed through the risk management process to effectively minimise the risk to the Institute's strategic objectives and/or the risk of non-compliance with obligations. The tolerance of risk in the Institute's strategic objectives may require acceptance, transfer (using, for example, insurance), mitigation, or avoidance of the risk. Compliance risks are not only risks of non-compliance, but also specific incidents/events that are particular to an act or policy that would have an adverse effect on the Institute.

For further details on the risk management process, please refer to the Risk Management Framework.

2.3.1. Identifying and Analysing Compliance Risk

Compliance risks are identified, then all contributing factors or causes and consequences are recorded in the risk register of the institute. An analysis is then undertaken to establish the impact and likelihood of the compliance risk occurring, using the Risk Assessment Matrix, and assuming no controls are in place to mitigate the risk. Once the impact and likelihood ratings have been generated, using the criteria in the Risk Assessment Matrix, the highest impact and likelihood rating are used to form the inherent risk rating.

The controls for the risk then need to be assessed for effectiveness in mitigating the risk, using the Risk Assessment Matrix. Based on this rating and the information regarding the controls, the impact and likelihood need to be re-assessed. The new highest impact and likelihood ratings form the residual rating.

The residual risk rating is then compared to the tolerable risk rating to determine whether treatment is required. Using the Institute's Risk Assessment Statement, tolerable risk ratings are able to be assigned for all risks which indicate the level of risk the Institute is willing to accept for that particular risk. Tolerable risk ratings are aligned with the Institute's overall risk tolerance, enabling it to fulfil its objectives and make more informed decisions. The Institute's risk tolerance is reflected in the Risk Assessment Statement that is part of the Risk Framework.

2.3.2. Evaluate and Treat Compliance Risk

Using the two risk ratings, tolerable risk and residual risk ratings, it then needs to be determined how the risk will be managed and whether risk treatment is required. Risk treatment enables an evaluation of how the identified risks will be treated (if necessary). If the residual risk rating is the same as the tolerable risk rating then no further action is necessary as the risk is already at an acceptable level. If the residual risk rating is higher than the tolerable risk rating, then action is required, and treatment plans must be put in place to mitigate the risk further and reduce the residual risk rating to the tolerable level. If the residual risk rating is lower than the tolerable risk rating, then an analysis of controls is to occur to check if there are too many controls to mitigate the risk. There might be controls that can be removed due to the high efficiency of other controls.

Selecting the most appropriate risk treatment involves balancing the costs and effort of implementation against the benefits derived. The treatment would also need to be assessed to ensure that it is workable within the wider operations of the Institute and does not create issues or duplication with other areas.

The strategies to manage risk can typically include transferring the risk to another party (e.g. insurance), avoiding the risk (e.g. not undertaking the particular operation / activity at all), reducing the negative

effect or probability of the risk, or even accepting some or all of the potential or actual consequences of a particular risk. It is important to note, however, that legislative requirements need to be observed when deciding on the most appropriate risk management strategy.

To reduce risk, treatment plans are used. Every treatment plan requires a person who is responsible for implementing the plan and an approver who ensures that the plan has fulfilled its objectives and is working efficiently to mitigate the risk. A treatment plan contains actions, which are required to mitigate a risk, that usually either reduce the impact of the risk or the likelihood or both.

For high and very high inherent risks, the Institute requires active management, regular monitoring and reporting to the Executive and Quality and Risk Committee. Medium and low risks are more tolerable, with the Institute requiring regular monitoring.

Once treatment plans have been implemented, adjustments are made to the risk register to appropriately reflect this. If there are any changes made as a result of treating the compliance risk that affect a compliance obligation(s), then these should be reflected in the relevant obligation within the annual compliance schedule.

2.3.3. Monitor and Review Compliance Risks

Compliance risks are reviewed by the Compliance, Quality and Risk Manager through annual risk register reviews. More frequent reviews of very high and high operational risks will occur, with a particular focus on the progress of mitigation strategies and treatment plans.

Annually a risk assurance review will include a review of existing risk ratings, identify new risks and review and validate the adequacy and effectiveness of existing risk controls / treatment plans.

2.4. Attestation Statement Process

On an annual basis all senior management complete an attestation statement. The attestation statement is a verification process undertaken to attest compliance with the obligations that are relevant to managerial areas. The attestation statement requires the signatory to confirm that any known breaches of legislation and Institute policies and procedures have been reported to the Compliance, Quality and Risk Manager. The statement is also used to confirm, to the best of the signatory's knowledge, that there are no irregularities leading to a negative impact (including fraud).

On an annual basis the Compliance, Quality and Risk Manager is required to undertake an internal audit of the Threshold Standards and the National Code using Institute templates. Within the template is provision to include a description of the evidence to support compliance with the standard and where action to remediate is required the register also includes provision to record this detail. The status of compliance with the Threshold Standards and the National Code will be attested to by the Compliance, Quality and Risk Manager.

Once the internal audits are completed a remediation action plan and continuous improvements are

recorded. A detailed report is developed for all relevant boards and committee detailing the identified non compliances, proposed remedial action and areas of priority for the next annual compliance schedule. The areas of non-compliance are then assessed for potential risk exposure.

3. Breaches and Breach Reporting

An important component of the Compliance Management Framework is to promote a culture at the Institute where compliance is valued and as such the reporting of compliance breaches is a critical element of this framework.

A breach or "compliance failure" is an act or omission leading to the Institute failing to meet its compliance obligations. A compliance breach can be unintentional or deliberate. It should be noted that deliberate or negligent breaches of the Institute's compliance obligations will not be tolerated, and offenders may be subject to disciplinary and/or legal proceedings (if appropriate).

All compliance failures are required to be reported, particularly those that are systemic and/or reoccurring issues. However, even a small failure, if not reported, can lead to the view that the failure does not matter or is not taken seriously, and this may result in non-compliance becoming a systemic problem.

All staff are encouraged to report breaches of the Institute's compliance obligations and other incidents of non-compliance. Through the identification and reporting of breaches, the Institute is able to identify systemic issues, address them and therefore improve its internal processes to ensure they are more robust. Reporting obligations are set out in the Risk and Compliance Management Policy and Procedure.

Breaches should be reported in consultation with the appropriate Manager/Executive Member, however, they may also be reported anonymously. Breaches are reported by completing the Reporting a Compliance Breach form available on the website.

Potential breaches may be identified from a number of sources including:

- reporting by staff
- the annual attestation process
- audit reports
- fines, penalties, damages or legal costs
- adverse publicity or media attention
- inquiries from regulators or other Government bodies
- allegations, complaints from stakeholders or whistleblowing reports
- death, injury or disability
- OH&S incidents
- systemic errors/problems

Where the breach reporting will lead to a conflict of interest for the Manager who should be consulted or the recipient of the report the breach report is to be sent to the CEO or Chair of the Board.

Figure 2 depicts the Institute's breach reporting process that will be followed by the Compliance, Quality

and Risk Manager when investigating and managing a reported breach.

The Institute's breach reporting process involves the following four stages:

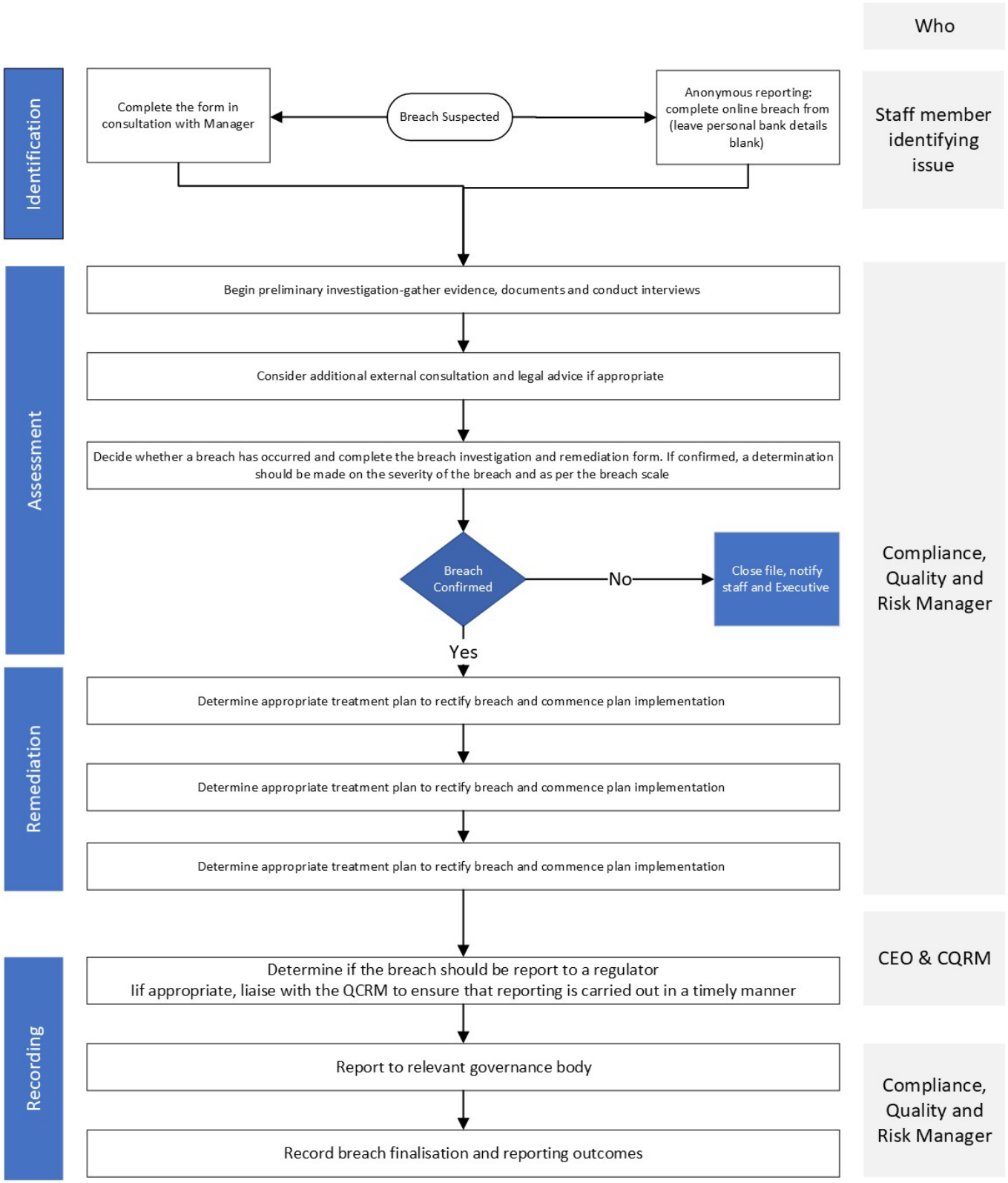
- **Identification**: a potential breach is identified and reported to the Compliance, Quality and Risk Manager.The online Compliance Reporting form should be completed in consultation with the Manager/Director (unless anonymity is required or the manager will have a conflict of interest).
- **Assessing**: the potential breach is assessed by the Compliance, Quality and Risk Manager who will assess the nature, scale and impact of breaches with reference to risk management protocols and determine the appropriate course of action.
- **Remediation**: a treatment plan will be developed and implemented to rectify the breach.
- **Recording**: the potential or actual breach must be recorded and all high risk actual breaches reported to the relevant governance body (Academic Board, QARC or Board of Directors). Where necessary actual breaches may be reported to a regulator or other external body if appropriate or required under legislation.

As part of the assessing stage, when a breach is confirmed, the severity (outcome) should then be assessed using the Breach Assessment Scale below:

Table 1. Breach Assessment Scale

Significant Breach		**Moderate Breach**		
Catastrophic	**Major**	**Substantial**	**Modest**	**Minor**
Loss of TEQSA registration, or other key license or accreditation loss; OR significant legal penalties or regulator sanctions against the Institute; OR criminal convictions resulting in imprisonment against BoD /staff.	Institute prosecution. OR BoD /staff member(s) are prosecuted without being imprisoned, OR Institute loses specific course accreditations or receives other license restrictions/sanctions which impacts on key operations, strategy and/or budget.	Institute prosecution. or BoD/staff being subject to legal proceedings resulting in only minor or no legal penalties; OR licensing restrictions/sanctions applied.	Institute receives warning or other notice from regulatory authority to rectify breaches and/or to undertake specified control improvements and/or additional reporting, without penalty applied.	Minor compliance breach incident or non-material series of small breaches, identified and rectified in-house. Correspondence from regulators acknowledging actions taken without further actions required.

Figure 2: Breach reporting process



4. Monitor and review

For compliance management to be effective, performance of the processes that make up the Framework are continually monitored and reviewed.

One such mechanism used to manage and monitor compliance activities across the Institute is the attestation process outlined above. However, this is an annual process and monitoring and review should be ongoing activities to be effective. The Executive for each area, is responsible for the continual monitoring of their area, review as necessary, and overall compliance profile and reporting of such to the Compliance, Quality and Risk Manager.

The Compliance, Quality and Risk Manager monitors the Institute's obligations register. As part of the risk management process, compliance risks are reviewed by the Compliance, Quality and Risk Manager through annual risk register reviews. More frequent reviews of very high and high operational risks, with a particular focus on the progress of treatment plans and the effectiveness of controls, take place as required.

The Institute's compliance obligations and compliance management processes and procedures contained within this framework are reviewed regularly by the Compliance, Quality and Risk Manager for currency and accuracy.

5. Compliance reporting

In line with the *Risk and Compliance Management Policy and Procedure*, the Compliance, Quality and Risk Manager coordinates the Institute's compliance reporting. The Compliance, Quality and Risk Manager will develop reports for:

- **Quality and Risk Committee:** The Quality and Risk Committee (QARC) exercises a governance role on behalf of the Board of Directors to ensure risk and compliance accountability is being properly exercised.The Institute's key compliance obligations (including any associated risks, controls, treatment plans and status updates) are reported to the QARC. Any identified new or emerging compliance risks, along with status updates on key compliance obligations and significant compliance breaches are also regularly reported to the QARC.
- **Executive:** The Executive receives regular compliance reports from the Compliance, Quality and Risk Manager, which are endorsed prior to each Quality and Risk Committee meeting. These reports include information on the Institute's key compliance priorities, any new and/or emerging compliance risks and significant compliance breaches.

6. Training

The Compliance, Quality and Risk Manager has oversight for the Institute's compliance training program. Some training is delivered by Managers/Executives. Training sessions on compliance management are provided by the Compliance, Quality and Risk Manager on a need's basis.

For any compliance training queries please contact the Compliance, Quality and Risk Manager.

7. Advice and Support

Please contact the Compliance, Quality and Risk Manager for any advice and support in relation to compliance management:

Website: **www.pia.edu.au**

Email: *policy@pia.edu.au*

Compliance Framework

Appendix A - Responsibilities and Accountabilities for Risk and Compliance Management

Staff at all levels are responsible for:

a) Developing an understanding of and applying sound risk management and compliance principals in their areas of work and embedding the Institutes risk management and compliance practices within general decision-making, operations, policies and procedures.
b) Promptly reporting any risk related issues, concerns, or incidents/events and compliance breaches to their supervisors / managers, who will escalate them to the Quality, Compliance and Risk Manager as appropriate.
c) Being aware of common areas of legislation, policy and procedure and appropriate professional standards that affect their day-to-day work and working relationships. Staff should also raise any concerns regarding issues and gaps as this will inform a robust risk and compliance training program.
d) Ensuring that their activities on behalf of the institute comply with the applicable laws and related Institute policies.

The Compliance, Quality and Risk manager is responsible for:

a) Developing and maintaining the Institute's risk management and compliance management framework and standards (including breach reporting), providing technical risk management and compliance support and training and associated tools and practices.
b) Reporting to the QARC on all aspects of both the risk and compliance framework, including academic risk and compliance issues.
c) Compiling a risk and compliance profile, including strategic and operational risks and compliance obligations for Executive and QARC reporting.
d) Providing other relevant risk and compliance information to the Quality and Risk Committee and/or Executive (e.g. breach reporting trends, incidents etc.).
e) Coordinating and supporting the establishment, ongoing maintenance and update of risks and compliance obligations.
f) Developing, implementing, and maintaining a Risk and Compliance Assurance (control testing) Program (based on industry best practice), covering all risk and compliance obligations
g) Coordinating the attestation process, breach reporting and any associated actions. Assisting areas to address issues in relation to breaches for rectification and continuous improvement.
h) Receiving advice regarding compliance obligation changes and ensuring the relevant area is notified accordingly.
i) Identifying new and amended compliance obligations and consulting with relevant areas on their applicability.
j) Ensuring that the Institute's compliance profile is reviewed annually.
k) Reviewing all business cases, contracts over $400,000 and insurance waiver requests from a risk perspective.
l) Ensuring controls to manage risks and compliance obligations are in place and operating as expected, including performance of self-assessment reviews and/or monitoring procedure.
m) Ensuring that recorded information regarding risk and compliance is completed and accurate.
n) Developing and delivering targeted risk and compliance training as required.
o) Co-ordinating the treatment plans including identification of the treatment plan and the appropriate stakeholders required, and the completion and monitoring all required tasks for the treatment plan.
p) Reviewing and making approved changes to the compliance obligations register on a regular basis. b) Ensuring all compliance issues are identified and included in their compliance obligations registers.
q) Act on any compliance breaches identified by, or notified to, them in accordance with this framework, and participate in any breach investigation activity as required

The CEO and Executive are responsible for:

a) Providing leadership and demonstrating commitment to the Institute's Risk and Compliance Management Frameworks.
b) Ensuring that risk management is incorporated in the University annual planning cycle.
c) Maintain an active oversight of the Institute's risk and compliance profiles (including ownership of strategic risks).
d) Reviewing the Risk Assessment Statement annually.

e) Ensuring risk assessments are undertaken in relation to all material projects and initiatives, and that all material functions, procedures, systems, programs, business activities within their areas of responsibility are subject to periodic risk review.
f) Ensuring a risk register and a compliance obligations register are established and maintained.
g) Ensuring treatment plans are implemented.

The Academic Board is responsible for:

a) Oversight of all academic governance risks

The Quality and Risk Committee:

a) Provides oversight of the institute's Risk and Compliance Management Frameworks.
b) Endorses amendments to the Institute's Risk and Compliance Policy and Risk Assessment Statement, which will be reviewed annually.
c) Reports annually to the Board of Directors on the status of the risk and compliance programs and associated outcomes.
d) Is invited to endorse the CEO's annual attestation statement.

The Board of Directors is responsible for:

a) Overseeing and monitoring the assessment and management of risk across the Institute and approving the Institute's Risk Assessment Statement
b) Ensuring the Institute fulfils its legal obligations and effectively manages any risk exposure resulting from any legal compliance failures.