Compliance Management Framework

Managing Compliance at the University

Risk and Compliance Office
Effective from 07-10-2014

Contents

Figures

Please note that the BWise risk and compliance management software will be live shortly. Whilst transition from current systems to the software occurs, the principles and processes of compliance management written in this framework will still apply. For any queries regarding the transition to BWise, please contact the Risk and Compliance Office.

1 Compliance Management Framework

The University is an agile and multi-faceted organisation that requires a compliance management framework that supports this operating premise without creating a "red tape environment".

Compliance has important links to risk and given that the University's obligations with regards to compliance are constantly evolving, the University requires a compliance management framework that allows it to demonstrate appropriate standards of governance without over complicating the process.

The University's Compliance Management Framework is aligned to the *AS 3806–2006 Australian Standard: Compliance programs*. This is an internationally recognised standard on better practice compliance management for all types of organisations.

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 University's compliance obligations. The Risk and Compliance Management Policy, and the Compliance Management Procedure are available on the Guide.

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

The Risk and Compliance Office consults extensively with key contacts from the various Faculties, Institutes and other areas (FIOAs) that have more specialised knowledge relevant to their particular areas of expertise to ensure that there is a coordinated approach to compliance.

1.2 What is compliance?

For the purposes of 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 University's compliance obligations refer to the laws, regulations, codes, policies and procedures with which the University is required to comply.

1.3 Why is compliance management important?

The University has a range of obligations with which it is required to comply. The bodies, both internal (e.g. Audit and Risk Committee) and external (e.g. the Victorian Auditor-General), that govern the University's operations expect that the University is fully conversant with its obligations and risks able to demonstrate that it is meeting and managing these obligations in a consistent and appropriate manner.

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 practices aimed at keeping abreast of this evolution. Remaining well-informed regarding the University's compliance requirements and obligations, and ensuring that there are strategies in place

to guide the University and its staff on matters of compliance, is a vital task and one that is critical to the success of the University.

The development of a strategic, effective and consistent approach to compliance management is essential as it will assist to reduce and/or mitigate a range of risks, including financial loss and reputational damage.

1.4 Accountabilities and responsibilities

The Compliance Management Framework promotes a culture where compliance is valued and as such every University 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 University Council, who hold ultimate responsibility for compliance management and the Risk and Compliance Office which is responsible for oversight, guidance and advice on the broader compliance management process. Key responsibilities are outlined in Appendix B: *Responsibility and Accountability for Risk and Compliance Management*.

1.5 Compliance registers

Compliance registers are used to record the University's compliance obligations and to ensure that the University is able to effectively and consistently manage the risks associated with non-compliance. Compliance registers contain the results of the compliance management process and they document the identified compliance obligations, any associated compliance risks and controls and action plans to mitigate the risks, along with an assessment of the cause and consequence of these risks. Compliance registers are stored in the BWise software system.

A Compliance Obligation Owner and a Compliance Implementation Officer are determined for each compliance obligation, who have overall responsibility for managing compliance with obligations throughout the University. The most appropriate staff to hold these positions are determined by the University Executive and/or senior management, in consultation with the Risk and Compliance Office.

There are currently two tiers of compliance registers: the key compliance obligation register and the compliance obligation registers. In order to determine the appropriate tier, all compliance obligations are risk-assessed and prioritised according to their inherent risk ratings, consistent with the University's Risk Assessment Matrix and the Risk Management Procedure. Obligations with the highest inherent risk ratings form part of the key compliance obligation register.

Compliance risks are created for the obligations with the highest inherent risk ratings. These are linked to the University's risk register and inform the University's compliance priorities. All compliance risks are subject to the risk management process as prescribed by the Risk Management Procedure.

The key compliance obligation register is owned by the Executive and contains critical organisational compliance risks which will link directly to the strategic objectives outlined in the University's strategic plan — *LIVE the future: Agenda 2020*. Compliance obligation registers are maintained by the relevant Faculties Institutes and other areas (FIOAs) of the University and document specific localised compliance obligations. The compliance obligations and requirements contained within each FIOA's compliance obligations register inform the FIOAs compliance profile.

Compliance registers are continually reviewed and updated to ensure that appropriate and current obligations (and any associated risks) are recorded, along with the relevant key controls and the progress of action plans where appropriate. This continual review is also a chance to identify any new and emerging compliance obligations which should also be monitored.

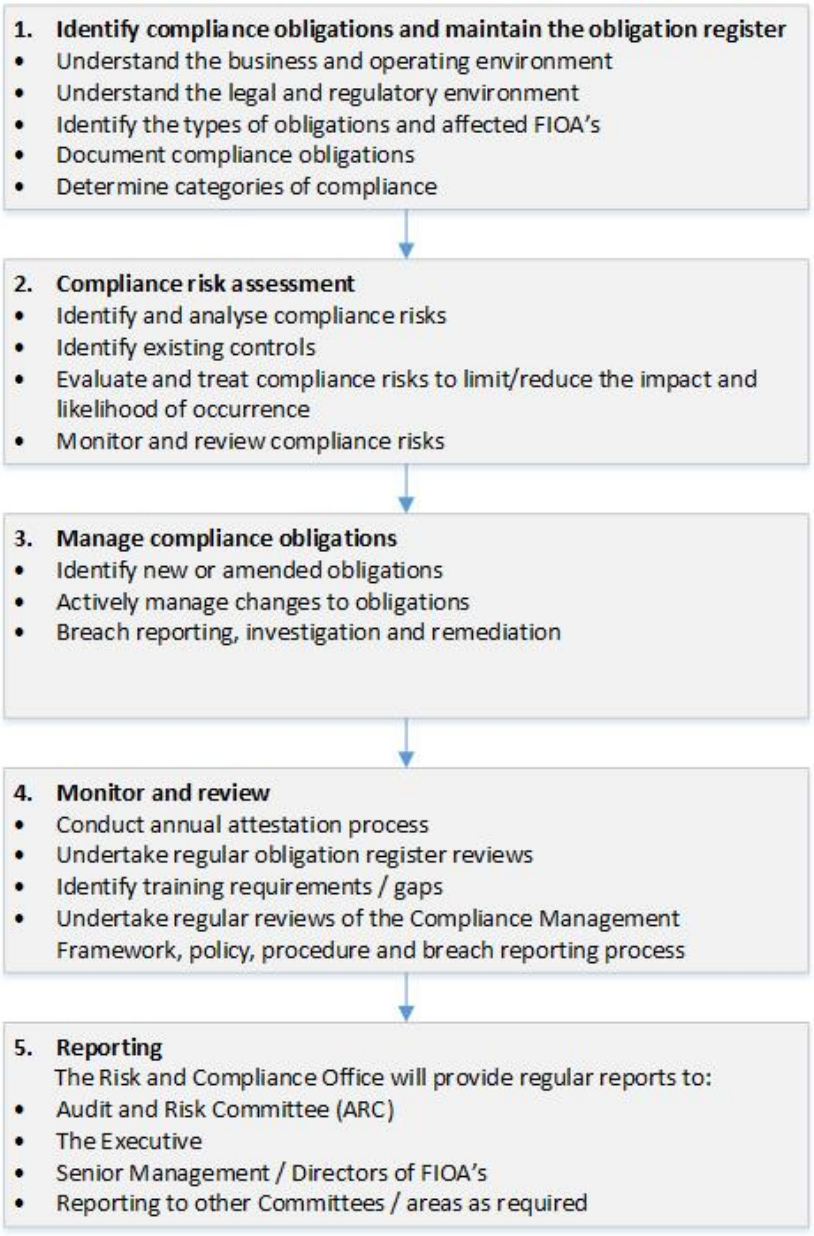
2 Compliance Management Methodology

2.1 Compliance Management Methodology

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

There is a standardised approach to the University's management of compliance and this process is aligned and consistent with the *AS 3806-2006 Australian Standard: Compliance programs*. The diagram below shows the five main stages in the compliance management process and these elements are described in further detail in the "Compliance Management Methodology" section of the Framework.

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



2.2 Identifying compliance obligations

The University has a wide range of compliance obligations including legislation, directives, permits, licences, orders issued by regulators, judgements of courts or tribunals, treaties, conventions, protocols and relevant industry codes and standards. The University 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 Risk and Compliance Office takes advice from the University Solicitor on any new/amended obligations affecting the University. This information is then distributed by the Risk and Compliance Office to the affected Compliance Obligation Owner and Implementation Officer who are responsible for advising the FIOAs.

To identify the compliance requirements and obligations that are applicable to a specific FIOA, the Risk and Compliance Office need to understand the FIOA's operations, what activities are undertaken by the FIOA, and what (if any) compliance management strategies are already in place.

In addition to an examination of University 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 management within the University. 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 University achieving its strategic objectives. Some of these risks will have the potential to have a major impact on the University and therefore may require more specialised attention. By expressing these risks as compliance risks, it allows the University to more closely monitor the obligation and to ensure that any negative impact is minimised.

All key compliance obligations are managed through the risk management process to effectively mitigate the risk — to the University's strategic objectives and/or the risk of non-compliance with obligations. 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 University

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 main effected FIOA. 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 Risk Assessment Matrix, tolerable risk ratings are able to be assigned for all risks which indicate the level of risk Deakin is willing to accept for that particular risk. Tolerable risk ratings are aligned with the University's overall risk tolerance, enabling it to fulfil its objectives and make more informed decisions. Currently the University's risk tolerance is reflected in Schedule A of the Risk Assessment Matrix in the Risk and Compliance Management policy.

2.3.2 Evaluate and Treat Compliance Risk

Using the two risk ratings, residual and tolerable 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 University 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 University requires active management, regular monitoring and reporting to the Executive and Audit and Risk Committee. Medium and low risks are more tolerable, with the University 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 compliance obligation register.

2.3.3 Monitor and Review Compliance Risks

Compliance risks are reviewed by the Risk and Compliance Office 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.

Risk assurance reviews are conducted by the Risk and Compliance Office. The prioritisation of the risks to be in the assurance reviews are determined by the inherent risk rating, with higher rated risks and associated controls/risk treatment plans being reviewed more frequently than low and very low risks. Risk assurance reviews 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.

An annual assurance plan is created in conjunction with the Internal Audit Annual Plan, to avoid duplication and concentration in the same areas.

Please refer to the Risk Management Framework under the Risk Assurance section for more information on the University's risk assurance and risk assurance reviews.

2.4 Attestation Statement Process

On an annual basis all senior management at director level or higher 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 University policies and procedures have been reported to the Director Corporate Governance Risk and Compliance Services (CGRCS). 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) and that all government grants have been used according to the conditions with which the funds were given.

The person signing the attestation statement is required to consult with relevant staff within their operational area to ensure that the information on the statement is as accurate and as complete as is reasonably practicable.

All attestation statements are received by the Risk and Compliance Office, who then collate them and check for any reported irregularities. Any irregularities that are reported, are investigated by the Risk and Compliance and are escalated to the Director, CGRCS as appropriate. See below for further information on breaches and breach reporting.

3 Breaches and Breach Reporting

An important component of the Compliance Management Framework is to promote a culture at the University 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 University 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 University'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 University's compliance obligations and other incidents of non-compliance. Through the identification and reporting of breaches, the University 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 Policy and the Compliance Procedure.

Breaches should be reported in consultation with the appropriate Manager/Director/HOS/Executive Member, however, they may also be reported anonymously. Breaches are reported by completing the online form on the *Risk and Compliance website*.

The University's breach reporting process captures compliance breaches across the University. However, it should be noted that there are various areas of the University (listed below) who are effectively capturing and managing breaches according to their own agreed processes and procedures, and in light of this, the University's breach reporting system has been developed to ensure that:

a) breaches occurring outside of these specialist areas are captured and managed; and
b) mechanisms are in place to enable the areas of the University who are already capturing their own breaches to provide the Risk and Compliance Office with the necessary information to facilitate the regular and consistent reporting of all breaches to the Executive and Audit and Risk Committee (ARC).

Breaches relating to (or arising from):	**Captured and managed by:**
Fraud and corruption	Office of the Chief Financial Officer
Student Complaints	Student Complaints Office
Copyright	Library
Health, safety and wellbeing	Human Resources Division
Workplace relations and performance	Human Resources Division
Radiation	Deakin Research
Biosafety	Deakin Research
Animal ethics	Deakin Research
HDR student misconduct	Deakin Research
International compliance	Deakin International
Autonomous sanctions	Deakin International / Deakin Research
TEQSA	Quality and Standards
Internal Audit	Internal Audit Unit
Privacy	The Office of the University Solicitor

Equal opportunity, discrimination, sexual	Equity and Diversity

The University's breach reporting process will predominately capture breaches that fall outside of the above listed categories, however, it can also capture breaches related to the above list if anonymity is required and the relevant area does not have a process in place to ensure this. It should be noted, however, that if a breach report is received through the University breach reporting process that is related to one of the above listed areas, the breach will be forwarded to the relevant FIOA for investigation and management.

FIOAs capturing the above listed breaches are required to submit quarterly summary reports to the Risk and Compliance Office in relation to any moderate breach reports that they receive. Significant breaches should be reported to the Risk and Compliance Office as they occur, on a case-by-case basis. Refer to the Breach Assessment Scale below to determine whether a breach is moderate or significant.

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

- reporting by staff
- self-assessments by FIOAs
- 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.

In accordance with the *Protected Disclosure Act 2012 (Vic)*, the University has in place the *Protection of Persons from Detrimental Action Procedure*. The purpose of this procedure is to:

a. explain how and to whom a Protected Disclosure can be made about the University or any of its employees or contractors; and
b. summarise the University University's obligations if a Protected Disclosure is made about it or any of its employees or contractors.

Figure 2 depicts the University's breach reporting process that will be followed by the Risk and Compliance Office when investigating and managing a reported breach. The FIOAs listed above can use this process as a model when managing their own breaches.

The University's breach reporting process involves the following five stages:

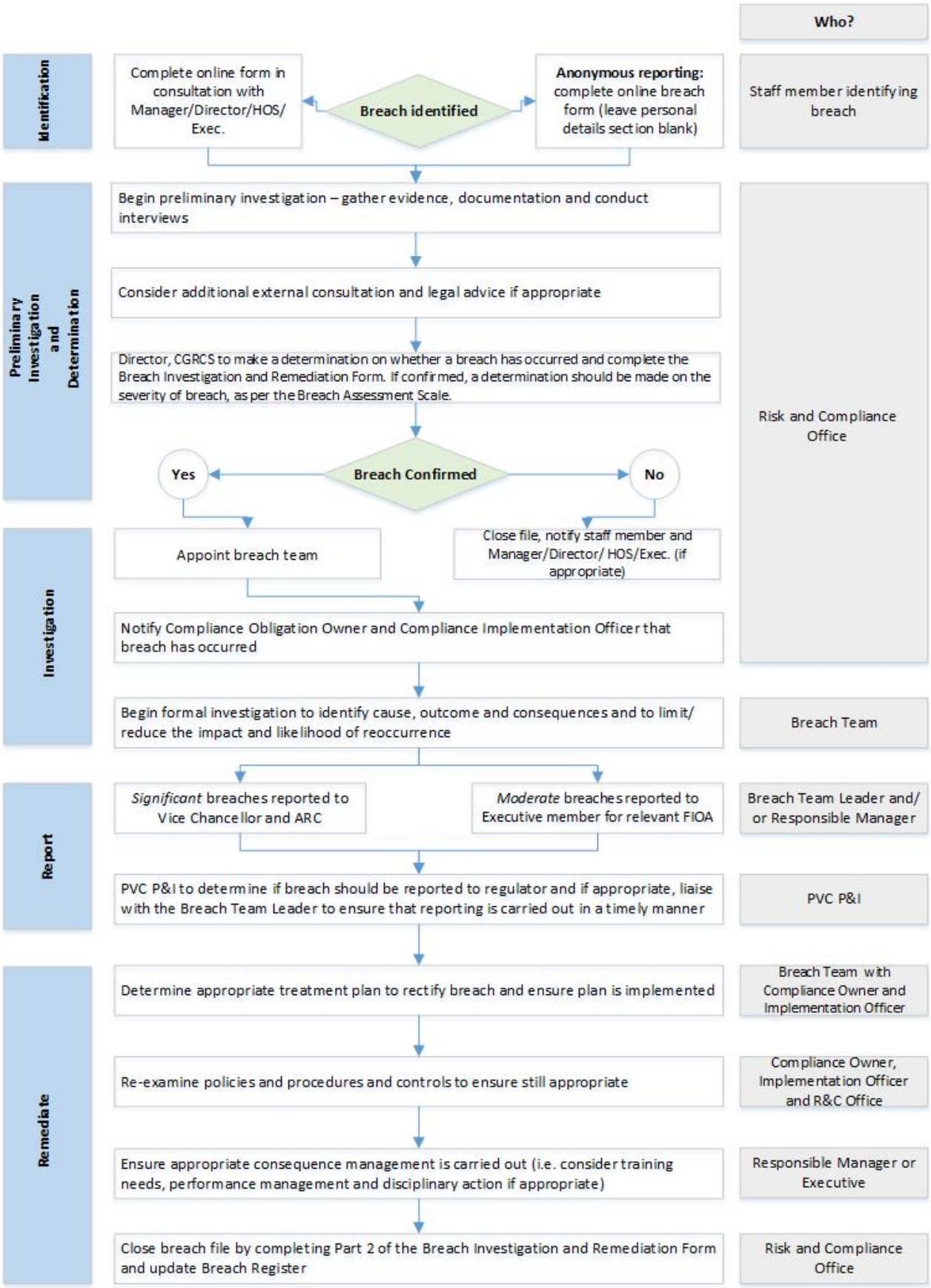
- **Identification**: a potential breach is identified and reported to the Risk and Compliance Office. The online Breach Reporting form should be completed in consultation with Manager/Director/HOS (unless anonymity is required).
- **Preliminary Investigation and Determination**: the potential breach is investigated by the Risk and Compliance Office before a determination is made by the Director, CGRCS regarding whether or not a breach has occurred who may consult with relevant staff during this determination.
- **Investigation**: after the breach is confirmed, a breach team is established and the formal investigation takes place.
- **Reporting**: the breach is escalated depending on the severity and nature. It may also be reported to a regulator or other external body if appropriate or required under legislation.

— **Remediation**: a treatment plan will be developed and implemented to rectify the breach.

As part of the preliminary investigation and determination stage, when a breach is confirmed, the severity should then be assessed using the Breach Assessment Scale below:

Significant Breach		**Moderate Breach**		
Catastrophic	**Major**	**Substantial**	**Modest**	**Minor**
Loss of TEQSA registration/license, or other key license or accreditation loss; OR significant legal penalties or regulator sanctions against the University; OR criminal convictions resulting in imprisonment against University Council / staff.	University prosecution; OR University Council / staff member(s) are prosecuted without being imprisoned; OR University loses specific course accreditations or receives other license restrictions/sanctions which impacts on key operations, strategy and/or budget.	University prosecution; or Council/staff being subject to legal proceedings resulting in only minor or no legal penalties; OR licensing restrictions/sanctions applied.	University 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 University is the attestation process outlined above. However, this is an annual process and monitoring and review should be ongoing activities to be effective. The Implementation Officers in each FIOA, in consultation with the relevant Compliance Obligation Owner, are responsible for the continual monitoring and review of their obligation register and overall compliance profile. The obligations registers are stored in the BWise system and Compliance Obligation Owners, Implementation Officers and senior staff in each FIOA have access to this system.

The Risk and Compliance Office monitors the University's obligations register. As part of the risk management process, compliance risks are reviewed by the Risk and Compliance Office 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 University's compliance obligations and compliance management processes and procedures contained within this framework are reviewed regularly by the Risk and Compliance Office for currency and accuracy.

5 Compliance reporting

In line with the *Compliance Procedure*, the Risk and Compliance Office coordinates the University's compliance reporting. The Risk and Compliance Office will develop reports for:

- **Audit and Risk Committee:** the Audit and Risk Committee (ARC) exercises a governance role on behalf of Council to ensure risk and compliance accountability is being properly exercised. The University's key compliance obligations (including any associated risks, controls, treatment plans and status updates) are reported to the ARC. 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 ARC.
- **Executive:** the Executive receives regular compliance reports from the Risk and Compliance Office, which are endorsed prior to each Audit and Risk Committee meeting. These reports include information on the University's key compliance priorities, any new and/or emerging compliance risks and significant compliance breaches.
- **Senior Management/FIOA Directors:** each senior manager/director of all FIOAs receives regular updates on the compliance obligations and/or compliance risks relevant to their area as well as any compliance breaches that may have occurred.

6 Training

The Risk and Compliance Office has oversight and organises a centralised University-wide compliance training program. Some training is delivered by Compliance Obligation Owner/Implementation Officers. Training sessions on compliance management are provided by the Risk and Compliance Office on a needs basis.

For any compliance training queries please contact the Risk and Compliance Office.

7 Advice and Support

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

Website: *https://wiki.deakin.edu.au/display/staff/Risk+and+Compliance*

Email: *riskandcompliance@deakin.edu.au*

Appendix A – Glossary of Terms

Attestation process: a verification process undertaken by all senior staff whereby they attest to compliance with the obligations that are relevant to their areas.

Compliance: adhering to the legislative requirements, organisational and industry standards, University policies and procedures and accepted community and ethical standards. Compliance is central to good governance.

Compliance breach: an occurrence of non-compliance with legislation, regulations, codes of practice and standards, as well as University legislation, policies and procedures.

Compliance Implementation Officer is accountable for:

a) 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.
c) The Compliance Implementation Officer is to be the main contact person for their area for all queries regarding compliance and are to escalate these as appropriate to the Risk and Compliance Office.
d) Co-ordinates 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.
e) The Compliance Implementation Officer is also to provide an explanation for any changes or delays to the treatment plan. Please note that for treatment plans, in the risk and compliance software BWise, the Compliance Implementation Officer is called 'Action Responsible'.

Compliance management framework: a document outlining all the relevant components and processes for compliance management across the University to ensure consistency of compliance management application.

Compliance management program: the totality of structures, including methodology, training, procedures and website that provide the foundation for the University's implementation, review and improvement of compliance management.

Compliance obligation: laws, regulations, codes, standards, policies and procedures the University is required to comply with.

Compliance Obligation Register: will identify the University's compliance obligations and risk assess the impact and likelihood of non-compliance. Key compliance activities and controls will be documented.

Compliance Obligation Owner is accountable for:

a) New and current risks and compliance issues being managed with the appropriate controls and treatment plans.
b) Ensuring controls to manage risks and compliance obligations are operating as expected, including performance of self-assessment reviews
c) Actioning breaches reported to them by their staff – identifying root cause and implementing appropriate corrective action (in consultation with the Risk and Compliance Office)
d) Ensuring that recorded information regarding risk and compliance is completed and accurate.
e) Approve all changes made to risk registers, ensuring that the information is accurate. Please note that for risk assessments the risk owner is also the 'approver' in the risk and compliance software. The 'approver' function may be delegated to another senior member of staff by the risk owner for operational risks.

f) Risk or Compliance Owners are to approve treatment plans, ensuring that they are implemented correctly and any changes made to them have been explained.

Compliance profile: description of a set of compliance obligations that can relate to the whole university, part of the university, or as otherwise specified. Will typically include some representation of the level/magnitude of the compliance obligations and associated risks involved.

Compliance risk: Compliance risks are specific incidents/events of non-compliance with requirements to a particular piece of legislation, or industry and organisational standards (including University policies and procedures) and codes that would have an adverse effect on the University.

Control: a measure, which could be one of or a combination of process, policy, device, barrier, practice, other actions established to alter the level of likelihood and/or consequence of the risk event.

Control rating: a rating that reflects the overall quality of the controls in place and their performance in changing (usually lowering) the inherent risk rating.

Impact rating: a rating showing the magnitude of the impact the risk would generate on the impact category.

Inherent risk rating: the level of the risk without any controls in place.

Likelihood rating: a rating indicating the likely frequency of the risk occurring.

Residual risk rating: the level of risk once controls have been established to alter the risk's likelihood or consequence.

Regulatory authority: any government body or other organisation responsible for regulating or enforcing compliance with legislative and other requirements (e.g.: Tertiary Education Quality and Standards Agency, TEQSA).

Risk: is the 'effect of uncertainty on objectives', as defined by Standards Australia and Standards New Zealand (*AS/NZS ISO 31000: 2009 Australian/New Zealand Standard: Risk management – Principles and guidelines*.) Risk is typically characterised by reference to potential events, and measured in terms of a combination of the likelihood of the event occurring and the consequence if it was to occur.

Risk assessment: overall process of risk identification, risk analysis and risk evaluation.

Risk management: coordinated activities, processes, and structures in place and undertaken to direct and control risk across the university. The risk management process involves the systematic application of management policies, procedures, and practices relating to the risk management activities of communicating, consulting, establishing context, and identifying, analysing, evaluating, treating, monitoring and reviewing risk.

Risk Management Framework: a document outlining all the relevant components and processes for risk management across the University to ensure consistency of risk management application.

Risk management program: the totality of structures, including methodology, training, procedures and website that provide the foundation for the University's implementation, review and improvement of risk management.

Risk tolerance: the amount of risk the University is willing to accept in pursuit of its strategic objectives in accordance with the University risk tolerance.

Tolerable risk: a risk rating indicating the maximum level of risk the University will accept for the associated risk. This is based on the University risk tolerance.

Treatment plans: treatment plans require actions that will reduce/mitigate the risk. It can involve avoiding activities that cause the risk, removing the source of the risk, changing factors driving either the likelihood and/or consequence, sharing or transferring the risk.

Appendix B — Responsibilities and Accountabilities for Risk and Compliance Management

Role	Responsibility / Accountability
Staff at all levels	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 University's 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 Risk and Compliance Office as appropriate. c) Being aware of common areas of legislation, University 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 University comply with the applicable laws and related University policies.
Compliance Implementation Officer	Compliance Implementation Officers are responsible for: a) 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. c) The Compliance Implementation Officer is to be the main contact person for their area for all queries regarding compliance and are to escalate these as appropriate to the Risk and Compliance Office. d) 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 e) Co-ordinating the treatment plan and is also required to provide an explanation for any changes or delays to the treatment plan. Please note that for treatment plans, in the risk and compliance software BWise, the Compliance Implementation Officer is called 'Action Responsible'.
Risk Administrator	Risk Administrators are responsible for: a) Reviewing and making approved changes to the risk registers through the BWise software on a regular basis. b) Ensuring all risk issues are identified and included in their risk registers. c) Being the main contact person for their area for all queries regarding risk management and are to escalate these as appropriate to the Risk and Compliance Office. d) Co-ordinates 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. The Risk Administrator is also to provide an explanation for any changes or delays to the treatment plan. Please note that for treatment plans, in the risk and compliance software BWise, the Risk Administrator is called 'Action Responsible'.
Risk Owner and the Compliance Obligation Owner	Risk Owners and Compliance Obligation Owners are responsible for: a) New, emerging and current risks and compliance issues being managed with the appropriate controls and treatment plans.

	b) Ensuring controls to manage risks and compliance obligations are in place and operating as expected, including performance of self-assessment reviews and/or monitoring procedures c) Actioning compliance breaches reported to them by their staff – identifying root cause and implementing appropriate corrective action (in consultation with the Risk and Compliance Office) d) Ensuring that recorded information regarding risk and compliance is completed and accurate. e) Approve all changes made to risk and compliance registers, ensuring that the information is accurate. Please note that the risk "owner" and the "approver" are two separate roles in the risk and compliance software. The 'approver' function may be delegated to another senior member of staff by the risk owner for operational risks. f) Risk or Compliance Owners are to approve treatment plans, ensuring that they are implemented correctly and any changes made to them have been explained. g) Developing and delivering targeted risk and compliance training to relevant areas of the University as required.
Project Managers	Project Managers are responsible for managing project risks and reporting on them to Deakin Portfolio Office
Director, Corporate Governance, Risk and Compliance Services	The Director Corporate Governance, Risk and Compliance Services is responsible for/has the oversight of: a) Developing and maintaining the University'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 ARC on all aspects of both the risk and compliance framework, including academic risk and compliance issues. c) Compiling a University wide risk and compliance profile, including strategic and operational risks and compliance obligations for Executive and ARC reporting. d) Providing other relevant risk and compliance information to the Audit 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 for all areas of the University. f) Developing, implementing and maintaining a Risk and Compliance Assurance (control testing) Program (based on industry best practice), covering all risk and compliance obligations across all Faculties Institutes and other areas of the University. 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) The Risk and Compliance Office receives advice regarding compliance obligation changes then we will ensure the relevant area is notified accordingly. i) In conjunction with the University Solicitor's Office, identify new and amended compliance obligations and consult with relevant areas on their applicability. j) In conjunction with the University Solicitor's Office, ensure that the University's compliance profile is reviewed annually. k) Reviewing all business cases, contracts over $400,000 and insurance waiver requests from a risk perspective. l) That all wholly owned entities are risk assessed bi-annually.
Deakin Portfolio Office	The Deakin Portfolio Office is responsible for the monitoring and reporting of all project risks to the Deakin Portfolio Board

University Solicitor	The University Solicitor is responsible for: a) Working with the Risk and Compliance Office to identify new and amended legislative compliance requirements. b) Providing advice to the Risk and Compliance Office in relation to legislative compliance matters when requested.
Vice Chancellor and Executive	The Vice Chancellor and the Executive are responsible for: a) Providing leadership and demonstrating commitment to the University'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 University's risk and compliance profiles (including ownership of strategic risks). d) Reviewing the Risk Assessment Matrix 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 risk registers and compliance obligations registers are established and maintained for their areas of responsibility. g) Ensuring treatment plans are implemented.
Audit and Risk Committee	The Audit and Risk Committee: a) Provides oversight of the University's Risk and Compliance Management Frameworks and associated programs. b) Endorses amendments to the University's Risk and Compliance Policy and Risk Assessment Matrix, which will be reviewed annually. c) Reports annually to the University Council on the status of the risk and compliance programs and associated outcomes. d) Is invited to endorse the Vice-Chancellor's annual attestation statement.
Academic Board	The Academic Board is responsible for: a) Oversight of all academic governance risks.
University Council	The University Council is responsible for: a) Overseeing and monitoring the assessment and management of risk across the University, including commercial undertakings and approving the University's Risk Assessment Matrix b) Overall responsibility for ensuring the University fulfils its legal obligations and effectively manages any risk exposure resulting from any legal compliance failures.