WESTERN SYDNEY UNIVERSITY

Strategic Priorities

Compliance Program Unit

2015-2018

Strategic Priority Drivers

Measurement against Compliance Institute’s Compliance Maturity Model (12 components).

Operationalising a proactive, agile, accountable culture that secures success.

Embedding a continuous improvement mindset with authentic behaviours within participatory decision-making.

Priority Focus Areas

Government Information (Public Access) Act 2009 (NSW)

Privacy and Personal Information Protection Act 1998 (NSW)

Defence Trade Controls 2012 (NSW)

Student Misconduct Rules

Maturing from Level 1 (Absent) to Level 2 (Reactive)

BUILD a compliance management framework

- Based on ISO 19600
- Identify obligations and assign accountability.
- Launch on the Enterprise-wide Risk and Compliance System.

DEVELOP policies and procedures

- Create Compliance Program Unit-owned policies, procedures, and Strategic Plan.
- Consult on and/or develop University-wide policies in areas of conduct, and specific operational legislative activities.

IMPLEMENT training and awareness

- Compliance Management Program and associated procedures.
- Mandatory training modules for all University staff.
- Specific legislation of interest

Strategic Priorities: 2015-2018
Focusses on *Development* and *Implementation*

Maturity Measurement

Current Level 1 - Absent (at 2015)	***Future Level 2 - Reactive (by 2018)***
There is no commitment to compliance management illustrated by no dedicated resources, no formal risk management policy and the absence of a compliance management program.	*There is commitment to address compliance management issues when major issues arise. There is no formal compliance management program but procedures and monitoring activities are put in place to prevent the reoccurrence of major issues.*

MATURITY → MEASUREMENT

Period of Measurement
September 2015 -
September 2018

Driver	Established Maturity Level at 2015	Steps to take to achieve next level of maturity	Maturity Level to Achieve by 2018
Component 1 Commitment by governing body and top management to effective compliance that permeates the whole organisation.	**Level 1 – Absent** Accountability for compliance does not exist. Compliance is simply not on the agenda of the governing body and top management. The structure for independent oversight does not exist.	Assign accountability of applicable legislation to operational units. The Compliance Program Unit (CPU) to present reports at least once a year to the Audit and Risk Committee (ARC) on updates on the Compliance Management Program (Program) and significant breaches if applicable. The CPU to continue to be a separate unit to operational units, and remain second line of defence.	**Level 2 – Reactive** Accountability for compliance is delineated at operational level. Compliance reaches the agendas of the governing body and top management when major breaches arise. The structure for oversight exists but is not independent.
Component 2 The compliance policy is aligned to the organisation's strategy and business objectives and is endorsed by the governing body.	**Level 1 – Absent** There is no clear compliance policy.	Publish the Compliance Policy for endorsement by the ARC. The Compliance Policy to focus on regulatory compliance rather than principles of conduct.	**Level 2 – Reactive** The organisation's compliance policy is primarily focused on legislative requirements. The organisation's governing body is aware this policy exists. The compliance policy is not referred to unless a breach or regulatory investigation occurs.
Component 3 Appropriate resources are allocated to develop, implement, maintain and improve the compliance program.	**Level 1 – Absent** No resources have been allocated to the compliance program.	The CPU must continue to have a senior FTE, which is the Compliance Program Manager (CPM). The CPM to consult with areas such as Procurement, Governance Services, Research to address compliance incidents in the GIPA Contract Register process, privacy, defence trade controls etc. Develop an incident reporting process.	**Level 2 – Reactive** Resources have been allocated to address areas where breaches have occurred. The record of effective implementation of suggested improvements to the compliance program is poor and/or not sustained. Staff or consultants may be engaged during time of crisis but are generally removed once the crisis is over.
Component 4 The objectives and strategy of the compliance program are endorsed by the governing body.	**Level 1 – Absent** The organisation's governing body does not consider compliance.	The Program should regularly report to the ARC as part of its endorsement journey.	**Level 2 – Reactive** Parts of the organisation's governing body have endorsed the compliance program.
Component 5 Compliance obligations are identified and assessed.	**Level 1 – Absent** The compliance obligations are seldom reviewed and there is no obligation register. Compliance-related decisions made are mainly based on gut-feel.	Identify the compliance obligations relevant to the University in consultation with the relevant operational units, and are reviewed annually.	**Level 2 – Reactive** The compliance obligations are documented and reviewed when compliance breaches become obvious and start to occur more frequently. The decision as to what the organisation's key compliance obligations are is made by those involved in that area. The decisions made are based mainly on the judgement of those managers impacted by the changes.
Component 6 Responsibility for compliant outcomes is clearly articulated and assigned.	**Level 1 – Absent** No responsibility for compliant outcomes is assigned.	Assign compliance obligations to the accountable operational unit when breaches occur for management and closure.	**Level 2 – Reactive** Responsibility for compliance is assigned when breaches occur.

MATURITY → MEASUREMENT

Period of Measurement
September 2015 - September 2018

Driver	Current Maturity Level at 2015	Steps to take to achieve next level of maturity	Maturity Level to Achieve by 2018
Component 7 Competence and training needs are identified and addressed to enable employees to fulfil their compliance obligations.	**Level 1 – Absent** Employees do not have the appropriate knowledge and skills to fulfil their compliance obligations. Training needs are very seldom assessed and no compliance training programs are offered.	Implement an email alert system on changes in legislative requirements for assigned laws to enable the University to fulfil and calibrate the fulfilment of its compliance obligations on a consistent basis. Onboard the privacy training module to the Enterprise mandatory training suite. Reported on the privacy training plan and monitored completion rates to the ARC. Consolidate separate training modules across different operational units (Procurement, Office of the General Counsel, and Records and Archives Management) with a unified message on GIPA provisions, and created new training modules where required. Create a network of compliance heads at NSW universities to enable and disseminate information sharing and effective benchmarking. Regularly disseminate communication and training on the obligations and Program from the CPU to University staff to increase and continue awareness and compliant culture on compliant behaviours and requirements.	**Level 2 – Reactive** Employees impacted by a breach are given training to fulfil their future compliance obligations. Training needs are usually identified as a result of a compliance breach or identification of new high risk areas. Some compliance obligations are circulated to staff i.e. via email, internal memos with no requirement for staff assessment on their understanding.
Component 8 Behaviours that create and support compliance are encouraged and behaviours that compromise compliance are not tolerated.	**Level 1 – Absent** No effort is made to create a culture of compliance. Non-compliant behavior is generally ignored and not monitored or discouraged.	Develop the Defence Trade Controls policy for the Research area. Embed expected compliant behaviours in the Code of Conduct policy. Collaborate with the Legal, Student Services, Campus Security to create Handbook Guide on the consolidation of the student misconduct policies and procedures under one new uniform rule and process.	**Level 2 – Reactive** Isolated efforts are made to encourage compliant behavior's when those areas are impacted by a breach. Policies may be created to fix a compliance problem when they occur but these policies are not enforced.
Component 9 Controls are in place to manage the identified compliance obligations and achieve the desired behaviours.	**Level 1 – Absent** No effective controls are in place to address compliance issues.	Consult with Procurement and Governance Services to improve the efficacy of the compliance controls of the contract register requirement under the Government Information (Public Access) Act 2009 (NSW) following an IPC desktop audit.	**Level 2 – Reactive** Effective controls are intermittently put in place in areas where compliance breaches have occurred.
Component 10 Performance of the compliance program is monitored, measured and reported.	**Level 1 – Absent** A compliance program does not formally exist nor is compliance performance monitored, measured or reported at all throughout the organisation.	Procure a reputable external vendor to design and implement the risk and compliance program.	**Level 2 – Reactive** Performance of the compliance program is only monitored where breaches have occurred. Breaches that occur in business units are not usually disclosed to senior management or reported to the governing body. Action may be taken to formally monitor, measure and report compliance performance if required by a regulator.
Component 11 The organisation is able to demonstrate its compliance program through both documentation and practice.	**Level 1 – Absent** Organisation is not able to either identify its compliance program or demonstrate its existence.	Create key compliance documents (Policy, Procedures, and Manual) to implement and operationalise the Program.	**Level 2 – Reactive** Organisation has insufficient record keeping regarding the program. Some policies, procedures and controls may be in place but there is no formal documentation or process for it to be properly demonstrated.
Component 12 The compliance program is regularly reviewed and continually improved.	**Level 1 – Absent** No formal compliance program or compliance procedures that exist are ever reviewed.	Create a 3-year Compliance Strategic Plan to embed and align the CPU's vision and operations to the University's, and the business and academic units where possible.	**Level 2 – Reactive** The compliance program is seldom reviewed except for when there is threat from regulatory intervention.