WESTERN SYDNEY
UNIVERSITY

SELF-ASSESSMENT
FACTSHEET

(Step 5 of the Workflow)

WHAT IS THE SELF-ASSESSMENT OF THE COMPLIANCE DIRECTORY?

Compliance Contacts must conduct a self-assessment of each assigned law on the Compliance Directory. The self-assessment involves:

- Self-assessing the *compliance status* of the specific obligations of the law;
- Confirming the details of the *internal controls* that mitigate the risk of non-compliance with the law; and
- Self-assessing the *residual risk* of each law.

For each law on the Compliance Directory, the Compliance Program Unit ("CPU") and the University General Counsel ("UGC") have assessed the impact and likelihood of the risk of non-compliance *before* any actions are undertake in order to prevent non-compliance from occurring. This is called the *inherent risk rating*, and will not change over time *unless* there is a major overhaul in the University or controlled entities' strategic and/or operation direction.

COMPLIANCE STATUS OF SPECIFIC OBLIGATIONS

Compliance Contacts are required to enter the specific obligations to which they must comply under their assigned laws. It should specify the *section* of the legislation, where possible. Compliance Contacts should maintain the *compliance status* of each obligation i.e. where compliant or non-compliant.

For any non-compliant (or partly non-compliant) obligation, a compliance incident **must** be reported on the Compliance Incident Reporting Register. See the *Compliance Incident Reporting* Factsheet for more information.

Compliance Contacts are **expected** to continuously review the obligations and the compliance status, especially if there are amendments to their assigned laws and/or significant changes to University operations.

The CPU has previously entered the key obligations on some laws. Compliance Contacts should continuously revise these obligations and update when necessary.

WHAT ARE INTERNAL CONTROLS?

Internal controls are the actions taken to prevent, detect, or correct incidences of non-compliance with the assigned law. These controls may be undertaken by the operating unit assigned the law. They may also be managed and/or created by the assigned operating unit for other areas/individuals to undertake to ensure compliance.

- *Preventative* controls are those actions put in place to avert an incident on non-compliance from occurring in the first instance. For example, ensuring individuals do not approve their own work (segregation of duties). These actions are conducted on a regular basis.
- *Detective* controls are intended to find incidences of non-compliance usually once they have occurred. For example, expiration tracking for chemicals to flag discrepancies between actual and expected outcomes (exception/reconciliation reporting).

- *Corrective* controls are designed to correct non-compliance incidents that have occurred with the view for it not to recur. For example, implementing a well-defined strategy to strengthen the level of resilience your operating area (business continuity plans).

Internal controls are likely to evolve over time – Compliance Contacts are **expected** to regularly monitor and update the list of controls, especially as a result of any significant changes to law and/or University operations.

Training can be both a preventative and corrective control. For more examples on types of controls, refer to the *Compliance Control Definitions* document accompanying this Factsheet.

WHAT IS RESIDUAL RISK?

Residual risk is the likelihood and impact of non-compliance *after* internal controls are deployed.

- The *impact* is an estimate of the potential losses associated with the risk of non-compliance. This includes financial (associated penalties or fines issued by the legislation's government authority), health and safety (injury or death), reputation (public confidence, media coverage), and legal (litigation, damages awarded, criminal and civil liability).
- The *likelihood* is the probability or chance of non-compliance occurring, whether it is rare, unlikely, possible, likely, or almost certain.

Compliance Contacts are **expected** to review, and reassess if necessary, the residual risk ratings of the laws that have updated or new controls.

This rating should be a *lesser rating* than the inherent risk rating assessed by the CPU and UGC.
The CPU has created a Customised Compliance Risk Assessment matrix which is used to assess both inherent and residual risk ratings. See the *Compliance Risk Assessment Matrix* document accompanying this Factsheet.

IS THERE TRAINING?

Yes. Training on the Compliance Management Program, of which the Compliance Directory forms part, is available as **MyCareer Online modules** that can be undertaken at any time.

Summary training is offered on the Compliance Management Program Yammer community, or e-updates.

CPU offers live training (via video conference or in-person) on the Program, which may be requested by individuals or invited by the CPU.

General information about the Compliance Management Program is also mentioned in the Manager Training, and Staff Induction training by the Talent, Learning, and Development unit.

OTHER FACTSHEETS

- Compliance Directory & Assignment Factsheet
- Legislative Alerts Factsheet
- Compliance Incident Reporting Factsheet
- Annual Attestation Factsheet