WESTERN SYDNEY UNIVERSITY

HOW TO MANUAL

Step by step guide to the
Compliance Management Program

FOR USE BY:

DESIGNATED COMPLIANCE REPRESENTATIVES & NOMINATED COMPLIANCE CONTACTS

read more on the compliance pages at https://www.westernsydney.edu.au/ougc/cpu

Contact Us

The CPU is located on Parramatta South campus,
Building EQ, Level 1.

Name	Email
Keira Hamilton *Director*	keira.hamilton@westernsydney.edu.au
Compliance *Shared mailbox*	compliance@westernsydney.edu.au

Welcome Message

Keira Hamilton
Director

Welcome to the Compliance Program Unit's "How To" Manual for the Compliance Management Program.

This Manual is intended for Designated Compliance Representatives and their Nominated Compliance Contacts.

It provides the essential information, step-by-step processes, and supporting resources required to enable these roles to effectively operate within the Compliance Management Program, and within the Enterprise Risk Management system in which it is hosted, to support and assure legislative compliance within their operating areas.

Whether you are new to the Program or already familiar with it, this Manual is designed as a practical, task-based resource.

You are encouraged to refer to the sections relevant to your role and responsibilities (clearly marked ★ throughout), and to return to this Manual as needed when undertaking compliance activities.

The CPU welcomes any questions or requests for support.

Our objective is to ensure a clear, efficient, and consistent approach to compliance attestation, enabling the University and its controlled entities to meet their assurance obligations with confidence.

TABLE OF CONTENTS

1. OBJECTIVES

OUTCOME OF PROGRAM IS TO ASCERTAIN THE RISK OF NON-COMPLIANCE WITH ASSIGNED LEGISLATION
I.E. IS IT WITHIN THE UNIVERSITY'S
RISK APPETITE OF "LOW"

WSU RISK MANAGEMENT FRAMEWORK

RISK RATING MATRIX

The risk rating matrix helps assess and prioritise risks based on their likelihood and consequence. Below is Western Sydney University's revised risk rating matrix and the corresponding definitions.

Risk						
Likelihood	Almost Certain 5	Medium 6	High 7	High 8	Critical 9	Critical 10
	Likely 4	Medium 5	Medium 6	High 7	High 8	Critical 9
	Possible 3	Low 4	Medium 5	Medium 6	High 7	High 8
	Unlikely 2	Low 3	Low 4	Medium 5	Medium 6	High 7
	Rare 1	Low 2	Low 3	Low 4	Medium 5	Medium 6
		Insignificant 1	Minor 2	Moderate 3	Major 4	Severe 5
		Consequence				

Likelihood

Likelihood describes the probability of a risk occurring within a given timeframe. The following categories provide a structured assessment of how often a risk is expected to materialise, ranging from frequent occurrences to rare or exceptional events.

No	Likelihood	Description
5	**Almost Certain**	The risk is expected to occur frequently, multiple times per year (76–100% probability).
4	**Likely**	The risk is likely to occur at least once per year under normal conditions (51–75% probability).
3	**Possible**	The risk may occur within a 1–5 year period but is not expected in most circumstances (21–50% probability).
2	**Unlikely**	The risk has a remote chance of occurring, generally within 5–15 years (5–20% probability).
1	**Rare**	The risk is highly unlikely, occurring only in rare or exceptional circumstances, less than once in 15+ years (<5% probability).

Risk Rating for Legislative Non-Compliance

Risk Rating	
Critical	Widespread, Enterprise-wide, systemic breach of legislation, or contracts, severely affecting WSU's ability to operate including government-mandated operational changes, or loss of accreditation or license. Litigation / prosecution resulting in criminal conviction or personal liability for executives or staff. Fines or claims exceeding $10 million. Regulatory investigation / commencement of criminal or civil proceedings. Severe reputational damage nationally and internationally.
Major	Breach of legislation, or contract with implications across various business units Potential legal disputes, including intellectual property, academic integrity, or corporate governance issues. Fines or claims between $1 million and $5 million. Civil action, or legal remediation required. Reputational damage with sector-wide awareness. Regulator issues infringement notices/enforceable undertaking to secure compliance by the University, or commences investigation
Medium	Low-level breach of legislation where compliance expectations are not fully met, with limited impact, and rectified through targeted management action. No legal consequences. No financial penalties, reputational harm, or operational disruption. Regulator issuing warning or Notice to Produce / Consent Order (or similar) to secure compliance
Minor	Low-level breach of legislation where compliance expectations are not fully met, with limited impact, and rectified through targeted management action. No legal consequences. No financial penalties, reputational harm, or operational disruption. Regulator issuing warning or Notice to Produce / Consent Order (or similar) to secure compliance
Insignificant	Administrative or technical non-compliance identified and rectified through routine processes. No regulatory investigation consequences or legal consequences. No financial penalties, reputational harm, or operational disruption. Maximum potential damages (~$5K) Regulator enquiry or information request, with no finding of non-compliance.

2. WHO DOES WHAT

1. Business — e.g. University staff, Business and Academic Unit heads

- **'Does' and owns compliance as part of their embedded business strategy, structure and operations.**

2. Compliance team — Director, Compliance

- **Subject-matter experts who ensure that compliance is 'done' (and properly).**

3. Audit — Internal audit, external auditors

- **Independent experts who check on the effectiveness of controls in place to address compliance risks.**

Three lines of defence

COMPLIANCE IS AN INDIVIDUAL & COLLECTIVE RESPONSIBILITY

Who does What in the Compliance Program at Western Sydney University

COMPLIANCE PROGRAM UNIT

Heads the strategy of compliance at the Enterprise-level& oversees the framework

- Monitors, configures & publishes the Directory
- Advises on & monitors some mandatory training for all staff
- Reports on the Program, training & breaches to internal/external offices
- Facilitates investigations of actual/potential breaches & attestations with Contacts & Representatives
- Reviews Compliance Policy & Program, and consults on other policies/ processes

COMPLIANCE REPRESENTATIVE

Typically Portfolio/Department-heads, & Deputy Deans who are accountable for particular operations/activities in the University

- Assigned Directory laws as it relates to their accountabilities
- Ensures all training in their area is completed & relevant training pertaining to their accountable operations is rolled out
- Ensures all actual/potential breaches of & in their area are promptly investigated
- Confirms the compliance attestations of their Compliance Contact/s
- Ensures relevant policies pertaining to their accountable operations are rolled out & maintained

COMPLIANCE CONTACT

Typically University management with specialist/ operational knowledge of particular operations/activities in their area (generally no lower than a HEW8)

- Assigned Directory laws as it relates to their knowledge of particular operations
- Monitors & annually reviews the Directory for changes to assigned laws & the key obligations
- Reports all actual/potential breaches of & in their area to the CPU
- Promptly investigates & remediates actual/potential breaches of & in their area
- Attests to compliance of & in their area
- Maintains procedures pertaining to their operational area

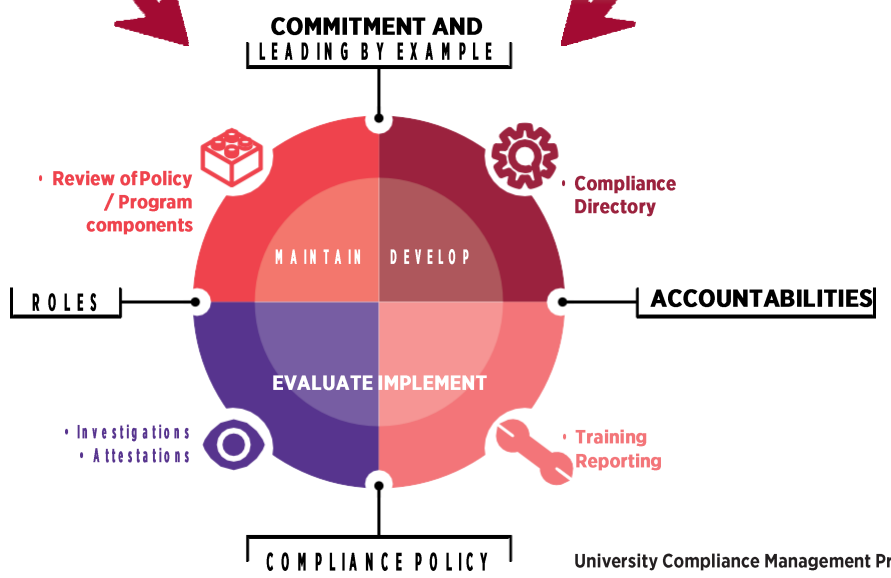
ALL STAFF

All University controlled entity employees including FT, PT, casuals & contractors

- Aware of, complies with & regularly consults the Directory
- Undertakes all mandatory & relevant training on time
- Reports all actual/potential breaches of which they are aware to an area's Compliance Contact
- Promptly remediates any actual/potential breaches as it relates to them
- Confirms their compliance to assist their area's Compliance Contact's attestation
- Adheres to University policies & procedures

ENABLE

ASSURE



University Compliance Management Program

COMPLIANCE SHOULD NOT CHANGE YOUR JOB.
IT IS EMBEDDED IN YOUR EVERYDAY POSITION.

The Compliance Program simply provides a formal, transparent & uniform framework to better assure of operational compliance across the University.

COMPLIANCE IS AN INDIVIDUAL & COLLECTIVE RESPONSIBILITY

RASCI chart of the Compliance Management Program at Western Sydney University

Term	Description
Responsible	Those responsible for the task, who ensures that it is done.
Accountable	The one ultimately answerable for the correct and thorough completion of the deliverable or task. There must be only one accountable specified for each task or deliverable.
Support	Resources allocated to *responsible*. Unlike *consulted*, who may provide input to the task, *support* helps complete the task.
Consulted	Those whose opinions are sought, typically subject matter experts; and with whom there is two-way communication. (Consultation may occur directly or indirectly through documented standards.)
Informed	Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.

**All staff includes all University staff as a whole, or staff within the Compliance Representative's operating area who may assist the Compliance Contact*

COMPLIANCE DIRECTORY

Task				
Notify about relevant laws in operating area	Consulted	Accountable	Responsible	Support
Add to and remove laws from the Directory	Accountable	Informed	Informed	Informed
Record legislation details including relevance to WSU	Accountable	Consulted	Consulted	Informed
Assess inherent risk	Accountable	Informed	Informed	Informed
Assign laws	Accountable	Consulted	Consulted	Informed
Record obligations *(self-assessment)*	Support	Accountable	Responsible	Informed
Confirm compliance status *(self-assessment)*	Support	Accountable	Responsible	Support
Record internal controls *(self-assessment)*	Support	Accountable	Responsible	*N/A*

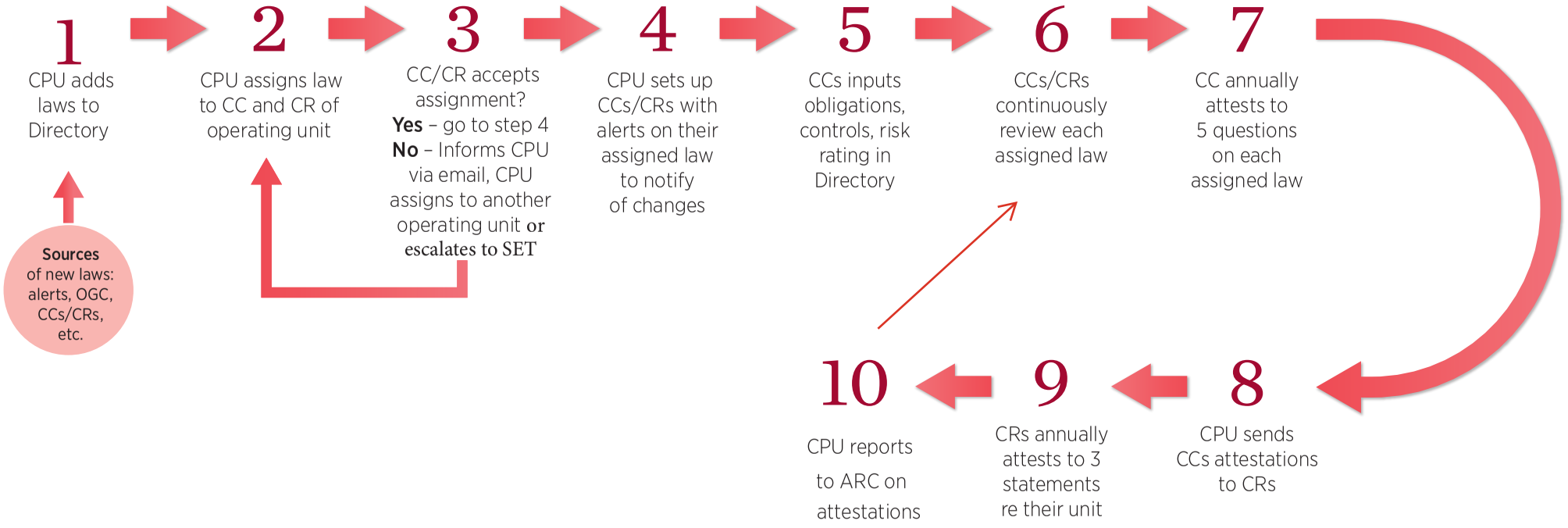
Assess residual risk *(self-assessment)*	Support	Accountable	Responsible	*N/A*
Updates documents (e.g. training, policy, procedures), groups (e.g. Senior Executive, Committees, staff), and self-assessment on law changes	Consulted	Accountable	Responsible	Informed Support

COMPLIANCE INCIDENT REPORTING

Task				
Report on potential / actual law, policy, and procedural breaches	Consulted	Accountable	Responsible	Responsible
Investigate breach reports including root cause analysis	Consulted	Accountable	Responsible	Support
Implementing corrective actions	Consulted	Accountable	Responsible	Support
Reporting on breaches to management and committees	Accountable	Consulted	Consulted	*N/A*
Maintain and triage breach register	Accountable	Support	Support	Support
COMPLIANCE ATTESTATIONS				
Maintain attestation registers and notifications	Accountable	Informed	Informed	*N/A*
Annually attest to all assigned laws on Directory	Support	Accountable	Responsible	Support

WESTERN SYDNEY
UNIVERSITY

UNIVERSITY COMPLIANCE DIRECTORY AND ANNUAL ATTESTATION PROCESS



Abbreviations
ARC – Audit and Risk Committee | **CPU** – Compliance Program Unit | **CC** – Compliance Contact | **CR** – Compliance Representative | **OGC** – Office of General Counsel

4. KEY DATES

Throughout the year, compliance network must continuously review their assigned laws and report any breaches to the CPU.

COMPLIANCE POLICY, CLAUSE 8

THE CPU REPORTS TO THE ARC *EVERY MEETING* ON COMPLIANCE INCIDENTS AND ISSUES

5. WORKFLOW DEEP DIVE
STEP 1 – ADDING LAWS

WHAT IS THIS?
The Compliance Directory sets out the NSW and Commonwealth legislation applicable to the University and its Controlled Entities.

Legislation may apply for a range of reasons, including the University's structure, operations, activities, revenue, or charity status.

The Directory captures only proactive obligations, being obligations that require the entity to take certain action or refrain from certain conduct.

The Directory also includes a Watchlist of instruments that may be relevant but are not currently captured as applicable obligations, such as legislation establishing authority, legislation awaiting assent or commencement, and relevant foreign legislation. For a full list of Watchlist categories, see page X.

WHO DOES THIS?
Compliance Program Unit.

WHAT DO THEY DO?
- Identify and maintain applicable legislation within the Compliance Directory.
- Assess and document the relevance of each legislative instrument to the University and its Controlled Entities (including The College).
- Determine enterprise applicability and the appropriate compliance management approach, including allocation of ownership.
- Assess the inherent risk associated with non-compliance.
- Allocate accountability to responsible operational units and assign Watchlist status where relevant.

WHEN DOES THIS OCCUR?
At any time during the calendar year.

How Compliance Contacts/Representatives can support:
Notify the CPU as soon as possible of any legislation that should be added to, amended in, or removed from the Compliance Directory or Watchlist.

STEPS 2 & 3 – ACCOUNTABILITY

WHAT IS THIS?
Each law in the Compliance Directory is assigned to the portfolio with accountability for managing compliance with that law, including the relevant operational compliance, controls, and procedures for the subject matter of the law.

Each law also has a designated Compliance Representative (that is, the accountable owner), who is usually the head of a portfolio.

The Compliance Representative nominates a Compliance Contact (that is, the subject matter expert), who is ordinarily no lower than HEW 9 and is usually a unit head.

WHO DOES THIS?
Compliance Program Unit.

WHAT DO THEY DO?

- Consult with the proposed designated area or areas, and with the University General Counsel where appropriate, before formally assigning accountability.
- Assign accountability for the law in the Compliance Directory, which triggers a system-generated automated email notification.
- Escalate any disagreement about the assignment of accountability to the Senior Executive Team via the University General Counsel for decision.

WHEN DOES THIS OCCUR?
At any time during the calendar year.

How Compliance Contacts/Representatives can support:
Promptly notify the CPU if an assignment of accountability is incorrect, and provide the name of the area that should be assigned accountability.

STEP 4 – EMAIL ALERTS

WHAT IS THIS?
Monitoring legislative change (including amendments, repeals, and new instruments) is a core requirement for maintaining operational compliance.

Unidentified or unmanaged legislative changes expose the University to an increased risk of non-compliance, which may result in regulatory action, penalties, and reputational impact.

To support this, legislative email alerts are established for each assigned law. These alerts ensure that the accountable area - through the Compliance Representative and Compliance Contact - has visibility of relevant legislative changes.

WHO DOES THIS?
Compliance Program Unit.

WHAT DO THEY DO?

- Register Designated Compliance Representatives and Nominated Compliance Contacts to the relevant legislative alert services for each assigned law.

WHEN DOES THIS OCCUR?
Immediately following the assignment of accountability.

How Compliance Contacts/Representatives can support:
Actively monitor assigned legislation by reviewing legislative alert notifications and taking appropriate action where changes impact compliance obligations.

STEP 5 – SELF-ASSESSMENT

WHAT IS THIS?
The self-assessment is the formal process used to identify, assess, and document the risk of non-compliance with assigned legislation.

It provides the evidence base demonstrating how compliance obligations are understood, controlled, and risk-assessed within the accountable area.

Self-assessment is not required for laws assigned as Watchlist items.

WHO DOES THIS?
Nominated Compliance Contact

WHAT DO THEY DO?
The self-assessment comprises four key activities:

- Identify and document the applicable compliance obligations under the assigned legislation.
- Assess and confirm the current compliance status of each obligation.
- Document the controls in place to mitigate the risk of non-compliance.
- Assess the residual risk of non-compliance, taking into account the effectiveness of those controls.

WHEN DOES THIS OCCUR?
Within 30 days of:
- assignment of accountability;
- a relevant structural change; or
- a legislative or regulatory amendment impacting the assigned law.

How the Compliance Program Unit can support:
Where possible:
- Review self-assessments for completeness and accuracy of identified obligations.
- Assess the design effectiveness of documented controls.
- Provide feedback on the appropriateness of the residual risk assessment.

STEP 6 – CONTINUAL REVIEW

WHAT IS THIS?
Ongoing monitoring and review of assigned legislation ensures the self-assessment remains current and supports an effective and efficient Annual Attestation process.

Failure to monitor and update legislative changes or non-compliance incidents may result in inaccurate compliance status and risk assessments.

The volume, severity, and management of non-compliance incidents - particularly where incidents are not appropriately addressed and closed - directly impact the overall residual risk of non-compliance.

WHO DOES THIS?
Nominated Compliance Contact

WHAT DO THEY DO?
- Monitor assigned legislation for relevant changes.
- Update the self-assessment (obligations, compliance status, controls, and residual risk) as required.
- Record and manage non-compliance incidents, including corrective actions and prevention measures.
- Implement and communicate any required changes to controls, processes, or training.

WHEN DOES THIS OCCUR?
At any time in response to:
- legislative or regulatory changes; or
- a non-compliance incident.

How the Compliance Program Unit can support:
- Assist in interpreting legislative alerts and their impact on compliance obligations.
- Provide guidance on required updates to controls, documentation, and communication pathways.

STEP 7 – COMPLIANCE CONTACT ANNUAL ATTESTATION

WHAT IS THIS?
Annual Attestation is the formal confirmation that the self-assessment and ongoing monitoring activities are current, accurate, and reflect the overall residual risk of non-compliance.

It provides assurance to the Board of Trustees via its Audit and Risk Committee, that there is no material non-compliance with assigned legislation that would adversely affect the University's ability to meet its legislative obligations.

WHO DOES THIS?
Nominated Compliance Contact

WHAT DO THEY DO?
Complete and submit the attestation, confirming the accuracy of the self-assessment, compliance status, and risk position.

WHEN DOES THIS OCCUR?
October to November, within the timeframe notified by the CPU.

How the Compliance Program Unit can support:

- Provide guidance on completing the attestation.
- Assist with system input where required.
- Issue reminders on key dates and completion deadlines.

STEP 8 – CPU VALIDATION

WHAT IS THIS?
Independent quality assurance of each annual attestation to validate the accuracy of the reported compliance status and residual risk of non-compliance.

WHO DOES THIS?
Compliance Program Unit

WHAT DO THEY DO?
- Review submitted attestations for completeness and accuracy.
- Validate reported compliance status and non-compliance incidents.
- Cross-check residual risk assessments against the compliance incident register.

WHEN DOES THIS OCCUR?
After submission of the Nominated Compliance Contact attestation and prior to the Designated Compliance Representative attestation.

How Compliance Contacts/Representatives can support:
- ARespond to CPU queries in a timely manner.
- Confirm and implement any required updates to attestations.

STEP 9 – *COMPLIANCE REPRESENTATIVE ANNUAL ATTESTATION*

WHAT IS THIS?
Compliance Representative Attestation is the formal confirmation of the overall compliance position across a portfolio, providing assurance that there is no material non-compliance risk.

It also reinforces segregation of duties by requiring independent oversight and confirmation of the position reported by Compliance Contacts.

WHO DOES THIS?
Designated Compliance Representative

WHAT DO THEY DO?
Review and attest to the portfolio-wide compliance position, confirming the accuracy of reported compliance status and residual risk.

WHEN DOES THIS OCCUR?
November to December, following CPU notification and provision of a summary of submitted attestations across the portfolio.

How the Compliance Program Unit can support:

- Provide guidance on completing the attestation.
- Assist with system input where required.
- Issue reminders on key dates and completion deadlines.

STEP 10 – ARC REPORTING

WHAT IS THIS?
Independent reporting to the Audit and Risk Committee (a sub-committee of the Board of Trustees) on the outcomes of the University's compliance framework, including key risks and assurance activities.

WHO DOES THIS?
Compliance Program Unit

WHAT DO THEY DO?
- Report on any assigned laws with residual risk above the University's risk appetite for legislative non-compliance (Low).
- Identify portfolios with outstanding attestations, noting that these revert to inherent risk ratings above appetite.
- Highlight any high-risk compliance issues identified through the attestation process and ongoing monitoring.

WHEN DOES THIS OCCUR?
In line with the annual reporting cycle, typically in Quarter 1 of the following calendar year.

How Compliance Contacts/Representatives can support:
Ensure all attestations are completed accurately and within the required timeframe.

INTERACTIVE LINKS FOR WORKFLOW STEPS

STEPS 2, 5, 6 & 7

COMPLIANCE CONTACTS

View your Assigned Laws and Annual Attestation Dashboard

STEP 4

LAWONE LEGISLATIVE EMAIL ALERTS

Log into LawOne

STEP 6

COMPLIANCE INCIDENT REPORTING

Report, manage, and view incident dashboard

STEP 9

COMPLIANCE REPRESENTATIVES

View Annual Attestation dashboard

6. PROCESS DOCUMENTS

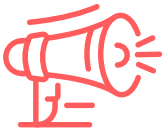
STEPS 1, 2 & 4

ASSIGNMENTS AND LEGISLATIVE EMAIL ALERTS

Pages 26-37

Inclusive of:

- Factsheets (Directory - pg 26-27, Legislative Alerts - pg 28-29)
- Watchlist Definitions - pg 30-31
- How to Login Instructions - pg 32
- How to Access Alerts Instructions - pg 33-35
- How to run a custom report on LawOne Instructions - pg 36-37



STEP 5

SELF-ASSESSMENT

Pages 38-54

Inclusive of:

- Factsheets (Self-Assessment - pg 38-39, Compliance Internal Controls - pg 40-44)
- How to Complete Compliance Self-Assessment Instructions - pg 45-52
- Compliance Controls Definitions - pg 53-54

STEP 6

COMPLIANCE INCIDENT REPORTING

Pages 55-62

Inclusive of:

- Factsheet (Incident Reporting - pg 55-56, Root Cause Methodology - pg 57-59)
- Incident Reporting Workflow - pg 60
- How to Report Non-Compliance Incidents Instructions - pg 61-62

STEPS 7 & 9

ANNUAL ATTESTATION

Pages 63-80

Inclusive of:

- Factsheet (Annual Attestation - pg 63-64)
- How to complete Annual Attestation for Nominated Compliance Contacts Instructions - pg 65-79
- How to complete Annual Attestation for Designated Compliance Representatives Contacts Instructions - pg 80

WESTERN SYDNEY
UNIVERSITY

UNIVERSITY COMPLIANCE DIRECTORY ASSIGNMENT FACTSHEET

(Steps 1-3 of the Workflow)

WHAT IS THE UNIVERSITY COMPLIANCE DIRECTORY (DIRECTORY)?

The Directory lists NSW and Commonwealth laws to which Western Sydney University ("University") and its controlled entities must comply.

Each law on the Directory is assigned to the relevant operating unit/s who are responsible and accountable for the compliance of the obligations within the legislation.

WHO GETS ASSIGNED LAWS ON THE DIRECTORY?

The Compliance Program Unit (**CPU**) notifies the operating unit's head (usually Director-level and above/Deputy Dean) of the law, and how it is relevant to the University and/or controlled entities. The CPU will ask the head to nominate a staff member with subject matter expertise as it pertains to the assigned law and the unit/s' actions on compliance with that law who will be the main point of contact. This includes actions on enabling compliance throughout the University and its controlled entities on the law.

The assigned operating unit head is called the "Compliance Representative" (**CR**). The nominated staff member responsible for complying with legislative obligations is nominated by the CR as the "Compliance Contact" (**CC**).

CAN I REFUSE AN ASSIGNMENT OF A LAW ON THE DIRECTORY?

It is not an option to opt out of legislative compliance that impacts the University and its controlled entities. However, you may refuse an assignment of a law on the Directory in the following circumstances:

i) you are <u>not</u> the operating area who has responsibility and accountability for compliance (or enabling compliance throughout the University and its controlled entities) with the law. You may have suggestions as to who it may be.

ii) the law is <u>not</u> relevant to the University or its controlled entities, or it has been repealed, <u>and</u> you are the correct operating unit that has the authority to state this.

Some laws are *shared* with other operating units, and some laws apply to different units in separate ways.

WHAT DO I DO ONCE I ACCEPT AN ASSIGNMENT OF A LAW ON THE DIRECTORY?

1. Record particular information about the law and the unit's compliance actions. See *Self-Assessment Factsheet* for more information.
2. Continuously review the law to keep the information current.
3. Action on alerts sent to you by the CPU regarding changes to the law. See *Legislative Alerts Factsheet* for more information. This includes updating documents and key controls as a result of any changes.
4. It is **imperative** to report on the Compliance Incident Reporting register of any incidences of non-compliance with the law. See *Compliance Incident Reporting Factsheet* for more information.
5. Attest annually to the above. See *Annual Attestation Factsheet* for more information.

Information that must be included are key controls to mitigate the risk of non-compliance with the law, self-assessment of the residual risk of non-compliance once controls are deployed, key obligations, and relevant policies, procedures, and/or training. See *Self-Assessment Factsheet* for more information.

WHAT HAPPENS IF I LEAVE THE ROLE/THE UNIVERSITY?

The CPU is notified of any role changes within and departures from the University and its controlled entities, and will update the assignment. It is best practice, however, to notify the CPU as soon as practicable so no delays are experienced which may impact the University and its controlled entities' compliance obligations.

Notifying the CPU as soon as practicable allows the CPU to reach out to the new incumbent to ensure they are trained and understand the requirements of the Compliance Management Program.

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

- Self-Assessment Factsheet
- Legislative Alerts Factsheet
- Compliance Incident Reporting Factsheet
- Annual Attestation Factsheet

WESTERN SYDNEY
UNIVERSITY

COMPLIANCE DIRECTORY AND LEGISLATIVE ALERTS FACTSHEET

(Step 4 of the Workflow)

WHAT IS A LEGISLATIVE ALERT?

Legislative alerts are customised email alerts sent to your Western Sydney University email account. It contains information on Parliamentary activity that are directly linked to full text legislation, Bills, and Explanatory Memorandum.

Designated Compliance Representatives and Compliance Contacts who are assigned laws on the University and controlled entities' Compliance Directory are automatically set up for alerts pertaining to their assigned laws. The Compliance Program Unit ("CPU") will send usernames and passwords to access the alerts for an assigned law once it is accepted.

Other University employees can request to receive alerts on particular laws.

WHAT DO I DO WHEN I RECEIVE AN ALERT?

Any changes to or affecting your assigned law is summarised in the body of the email. There is more detailed information to access, which requires you to login the alert database using the username and password sent by the CPU when you accepted the assignment of the law.

For instructions on how to login and access the detailed information on the database, refer to the *Legislative Alerts Instructions* document accompanying this Factsheet.

WHAT DO I DO WHEN AN ALERT CONTAINS CHANGES THAT AFFECT MY ASSIGNED LAW?

1. **Inform** a Senior Executive if appropriate.
2. **Consult** with immediate team and affected stakeholders including control functions such as the CPU, Office of General Counsel, Audit and Risk Assessment etc if necessary.
3. Update and/or create **internal documents** such as policies, procedures, Intranet pages, or training.
4. If appropriate, **communicate** to the rest of the University or controlled entities of the change and the updates made, as well as any actions they must undertake to ensure compliance.
5. Update / create the **obligation** in the Compliance Directory ("Directory"), and its compliant status.
6. Update / create **internal controls** pertaining to the change if necessary.
7. Reassess the **residual risk rating** of the law on the Directory.

For more information on Steps 5-7, refer to the *Self-Assessment Factsheet*.

CAN I CHANGE THE AMOUNT / FREQUENCY OF THE ALERTS BEING SENT TO ME?

As the default, Compliance Representatives are emailed a summary on the 1st day of every month *in the event* that any of their assigned laws have been amended. Compliance Contacts are emailed on the day that any of their assigned laws are repealed/amended/subordinate legislation is made.

Contacts can request to have a consolidated alert of all changes once a week or monthly instead of daily, however it recommended for Contacts to receive alerts either daily or weekly, as an important change may be missed while waiting for the 1st day of the next month. There is also an option to create a custom report on all changes at a particular point in time – refer to the *How to create a custom report* document accompanying this Factsheet.

The number of alerts, no matter the frequency, is based on the number of your assigned laws and whether they are amended by Parliament as whole (i.e. not by individual sections) – the CPU cannot control this.

CAN I SUSPEND THE ALERTS FOR A PERIOD OF TIME?

The CPU cannot suspend or stop the alerts to your email as it is a key feature of the Compliance Management Program ("Program") that demonstrates "completeness". If you are going on leave, you may request the CPU to alter the frequency of the email alerts during the leave period (monthly instead of daily for example).

Being on leave does not absolve you from your compliance obligations.

CAN I OPT OUT OF RECEIVING THE ALERTS?

No. The alerts are subscribed to you based on the laws assigned to and accepted by your area. These alerts are embedded into the Program, and are an important component. The Program regularly undergoes external and internal audits. If the laws are not appropriately assigned, contact the CPU.

The alerts assure that Compliance Representatives and Compliance Contacts are receiving *at least one* avenue of information that notifies of any changes that affect their assigned laws. You may sign up to multiple feeds, alerts, and notifications from other sources – there is no maximum number of sources to which you need to subscribe, but it is **expected** to subscribe to at least one, which is the alert service CPU subscribes you.

WHAT HAPPENS IF I LEAVE THE ROLE/THE UNIVERSITY?

The CPU is notified of any role changes within and departures from the University, and will update the assignment as well as the alert subscription. It is best practice, however, to notify the CPU as soon as practicable if you are leaving and to whom the alerts should be sent, if known, so no delays are experienced which may impact compliance obligations.

IS THERE TRAINING?

Yes. There is specific training on the legislative alerts conducted by the vendor/provider, LawOne of TimeBase. This usually occurs twice-yearly, ~February and ~July, via video conference. CPU notifies the compliance network on Yammer, and extends an invitation to join the video conference. Summary training is offered on the Compliance Management Program Yammer community, or e-updates.

OTHER FACTSHEETS

- Compliance Directory & Assignment Factsheet
- Self-Assessment Factsheet
- Compliance Incident Reporting Factsheet
- Annual Attestation Factsheet

Watchlist Reasons

Instrument specific: items 1-3 may be assigned to particular operating area/s, items 4-5 always should be.

1. It is a **Bill** awaiting to be enacted (as only current Acts of Parliament are listed on the Directory).
2. It is an Act that has **not yet commenced** (as only current Acts of Parliament are listed on the Directory).
3. It is an **international** law/instrument (as only Australian Federal and State laws are listed on the Directory).
4. It is a **subordinate** legislation enabled by a principal Act on the Directory, and contains numerous prescriptive obligations of which particular operating areas must be aware.
5. The law is applicable to the University/Controlled Entity and its operations but the law does **not impose a *direct* or *specific* obligation** onto the University/Controlled Entity for compliance.

5A. This law is applicable to the University/Controlled Entity and its operations but the law may set up **authority** or **formulation** only.

5B. This law is applicable to the University/Controlled Entity and its operations, and informs how to conduct **BAU procedures** when the event this Act is about occurs *without* imposing a direct or specific obligation.

5C. This law is applicable to the University/Controlled Entity and its operations but the law may be a **voluntary** instrument.

University specific – currency of operations: items 6-7 may be assigned to particular operating area/s.

6. The law is applicable to the University/Controlled Entity and its ***potential* (but not current)** operations.

6A. The law is applicable to the University/Controlled Entity and its ***potential* (but not current)** operations, and is subject to an **annual review** of applicability.

7. The law is applicable to the University/Controlled Entity and its operations but it **does not have any *current* activities** or situations (more than 10 years when a relevant situation occurred).

Operational unit specific – accountability of operations: – items 8 should be assigned to particular operating area/s, and always is an active assignment to the operating area/s who has operational legislative compliance accountability.

8. For awareness purposes only for particular operating areas **not directly involved** in or solely accountable for operational compliance of legislative obligations but it affects their operations, or execution and/or implementation of mitigating controls.

Enterprise and operational unit specific – applicability of operations: item 9 may be assigned to particular operating area/s.

9. The law is not applicable to the University/Controlled Entity because of particular reasons of its **operations** or it has an **exemption**.
   The University/Controlled Entity may follow it for best practices reasons only.

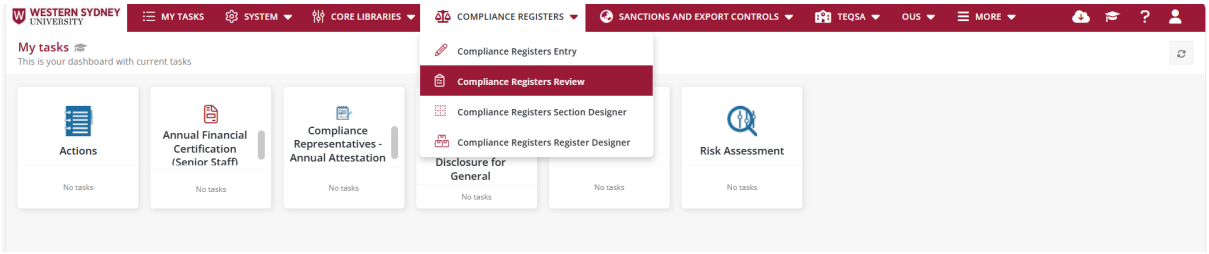
Awaiting

10. The law is awaiting **SEC strategic decision** to trigger applicability / **OGC interpretation** for applicability.
11. The law is applicable to a *Controlled Entity* whereby an operating portfolio in the *University* is accountable for executing operational compliance / custodianship of Enterprise-wide controls on behalf of the controlled entity.

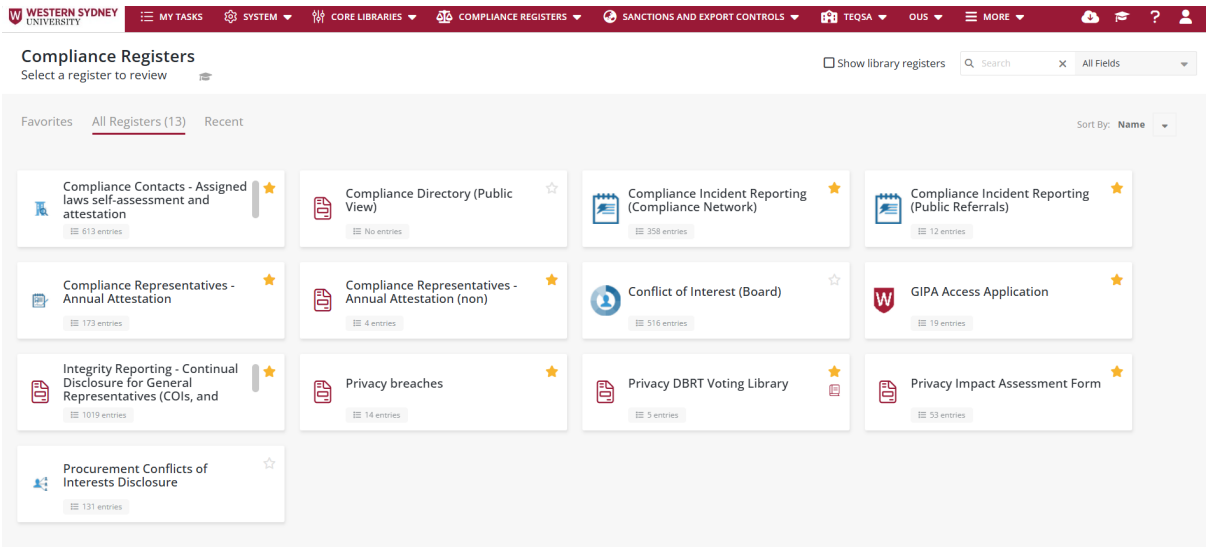
Logging into Western.ERC platform

1. Access https://erm.protecht.com.au/wsu
2. Enter your Western credentials for single sign-on login
    a. MFA to access

3. Access on the top menu ribbon “Compliance Registers”
4. Choose “Compliance Registers Review” from the drop down.



5. Choose the relevant register.



Legislative Alerts Instructions

Receiving alerts

Sender and Recipients

1. Emails alerts are sent from lawone@timebase.com.au.
2. Emails are sent to Compliance Representatives, Compliance Contacts, Compliance Program Unit, and other interested persons (seen in the "CC" field of the email).

Regularity

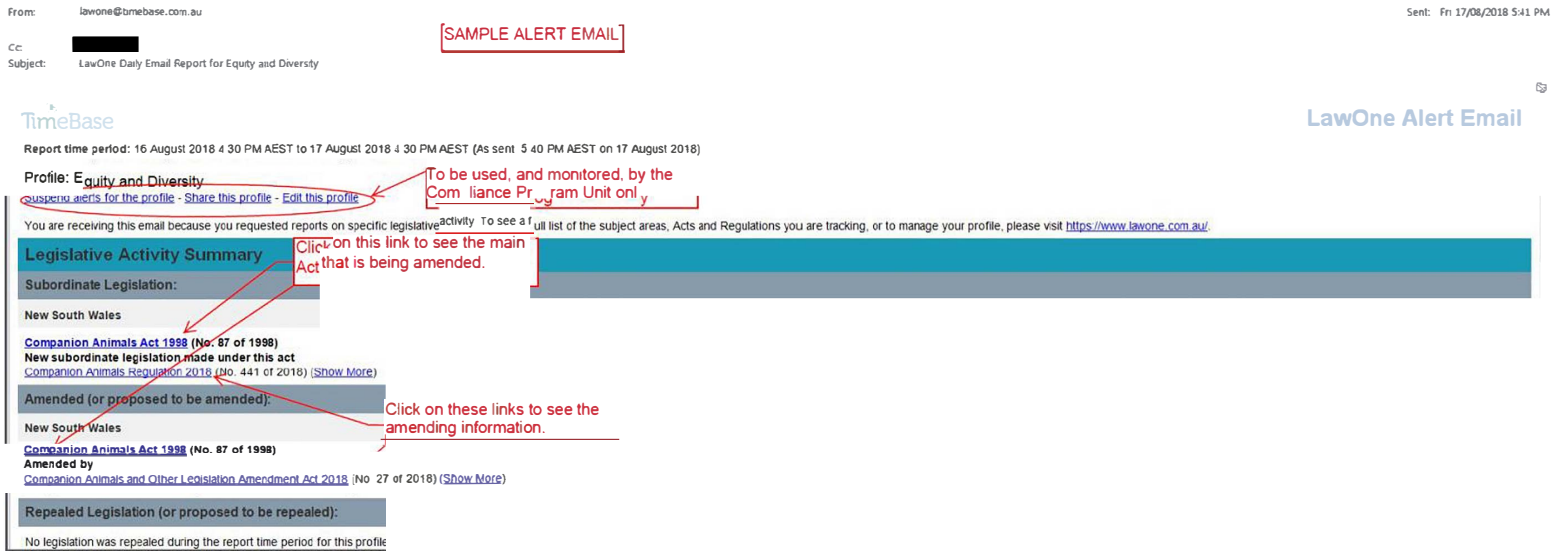
3. There is one alert per assigned law on the Compliance Directory, sent on the day of the amendment.

Content in the alert email

4. The alert is divided into summary sections of:
    a. Bill/Draft Progress - *not applicable to all laws; contact the CPU if this information is required*
    b. New or commencing legislation - *not applicable to all laws; contact the CPU if this information is required*
    c. Subordinate legislation
    d. Amended (or proposed to be amended)
    e. Repealed legislation (or proposed to be repealed)
    f. Legislative activity details
5. The summary sections outline the main Act being amended (the assigned law – in **bold font**), and the amending legislation (in unbolded font).
6. The Legislative activity details contain more information such as purpose, notification, and commencement dates.

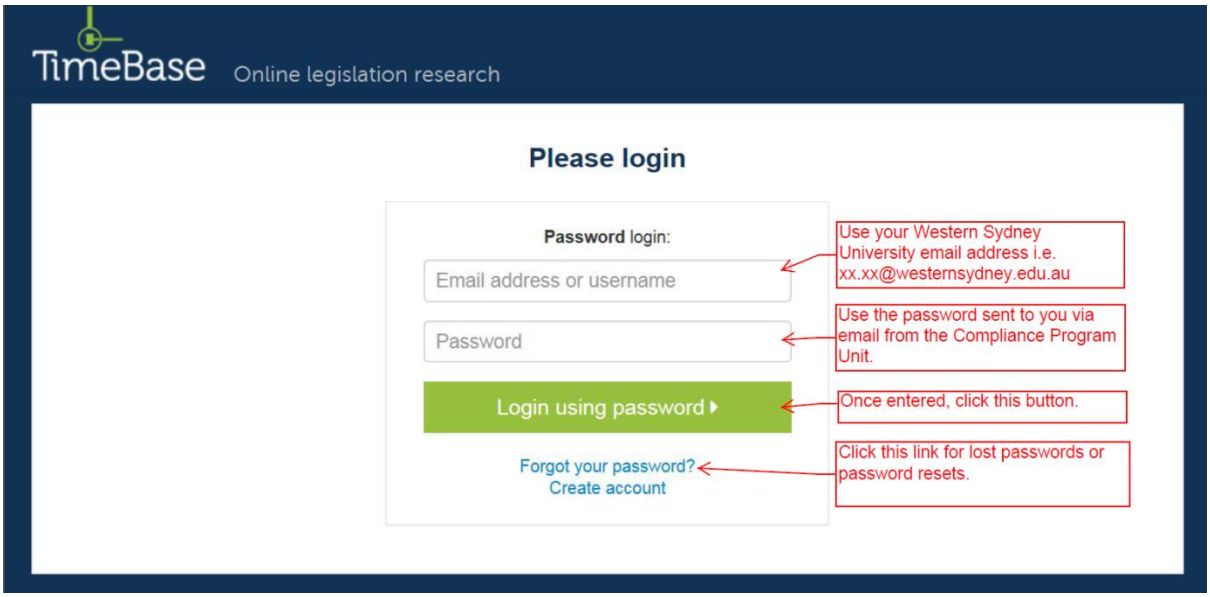
Accessing the amendment information in the alert email

7. For the most part, individuals will only want to access the amending legislation by **clicking the second link under the main Act to in unbolded font** – *see screenshot below.*
8. Clicking any of the links in the alert email will bring you to the log in page for TimeBase.



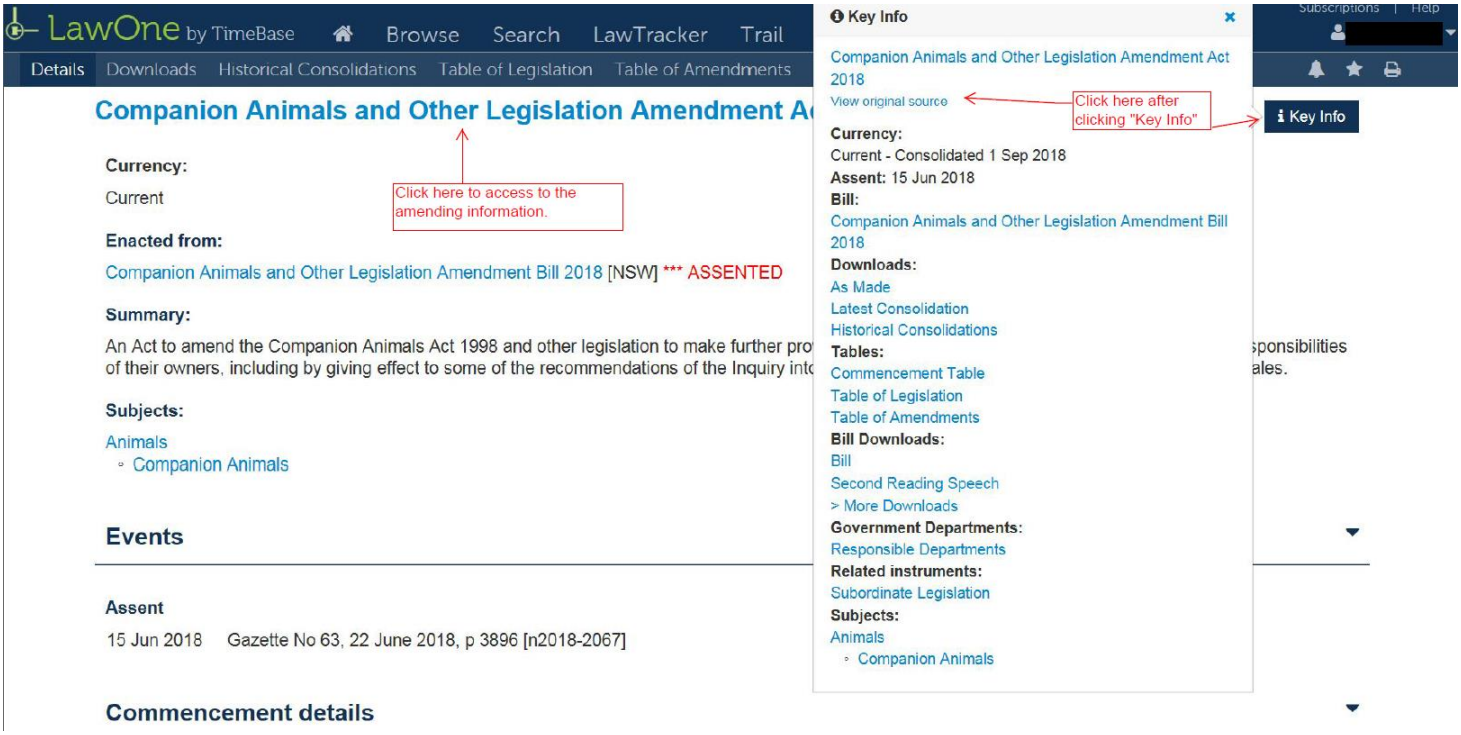
Logging into TimeBase

9. Enter your Western Sydney University email address in the “email address or username field”.
10. Enter the password sent to you via email from the Compliance Program Unit in the “Password” field.
11. Click “Login using password” to access the information.
    a. For any lost passwords or password resets, see the last section on “Passwords” below.



Accessing the amendment information from TimeBase

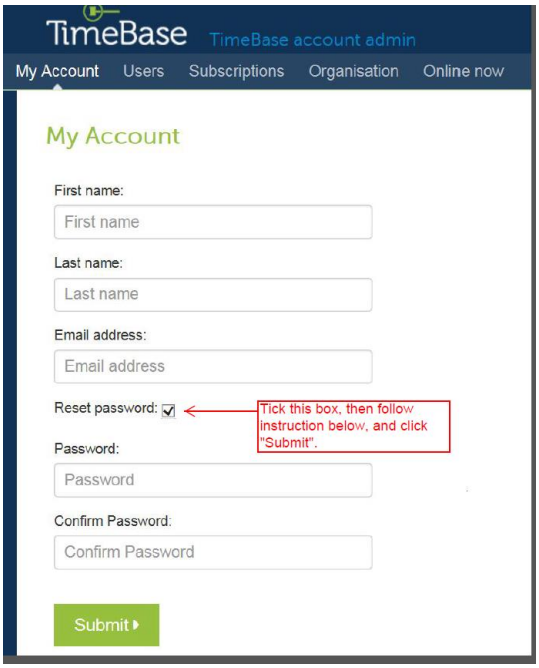
12. The login page will direct you to the page of the link you initially clicked on in the alert email (which should be the amending legislation).
13. The page will be a more detailed summary – it is recommended to see the original source of the amendment (i.e. the text of the amending legislation) by either:
    a. clicking the amending legislation name (if hyperlinked), or
    b. clicking the “Key Info” button, and then clicking “View Original Source”.



Passwords

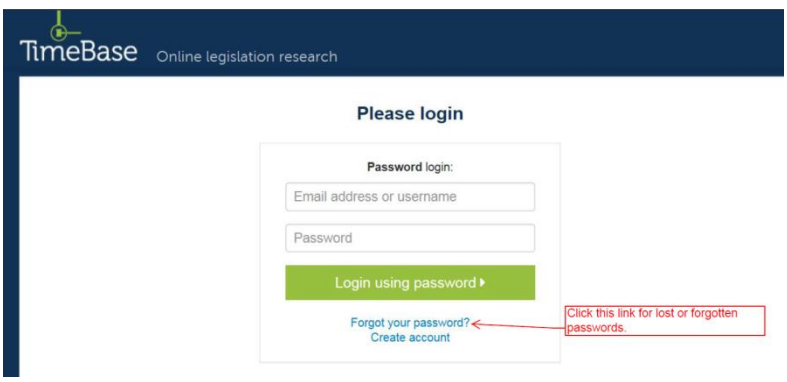
Password Resets

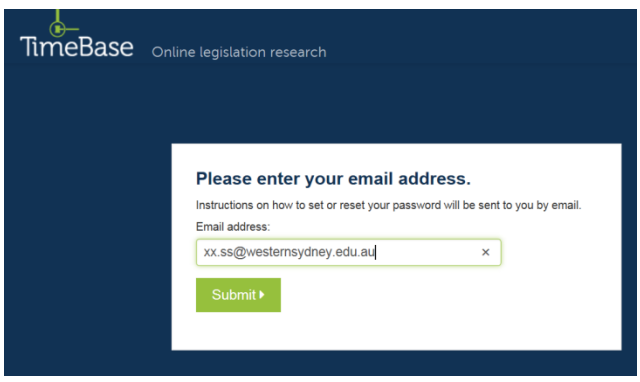
14. To reset your password while logged into TimeBase
    a. Click on the arrow next to your name in the top right hand of the page
    b. A window will open; click on “My Account” button.
15. Tick “Reset Password” box.
16. A window will open to enter and confirm a new password.
17. Click “Submit”.
18. You will receive a confirmation email stating your password has been updated.



Lost / Forgotten Passwords

19. If you have lost or forgotten your password when wanting to log into TimeBase, click “Forgot your password” link on the login page.
20. Enter your Western Sydney University email address to receive instructions via email on how to reset your password.

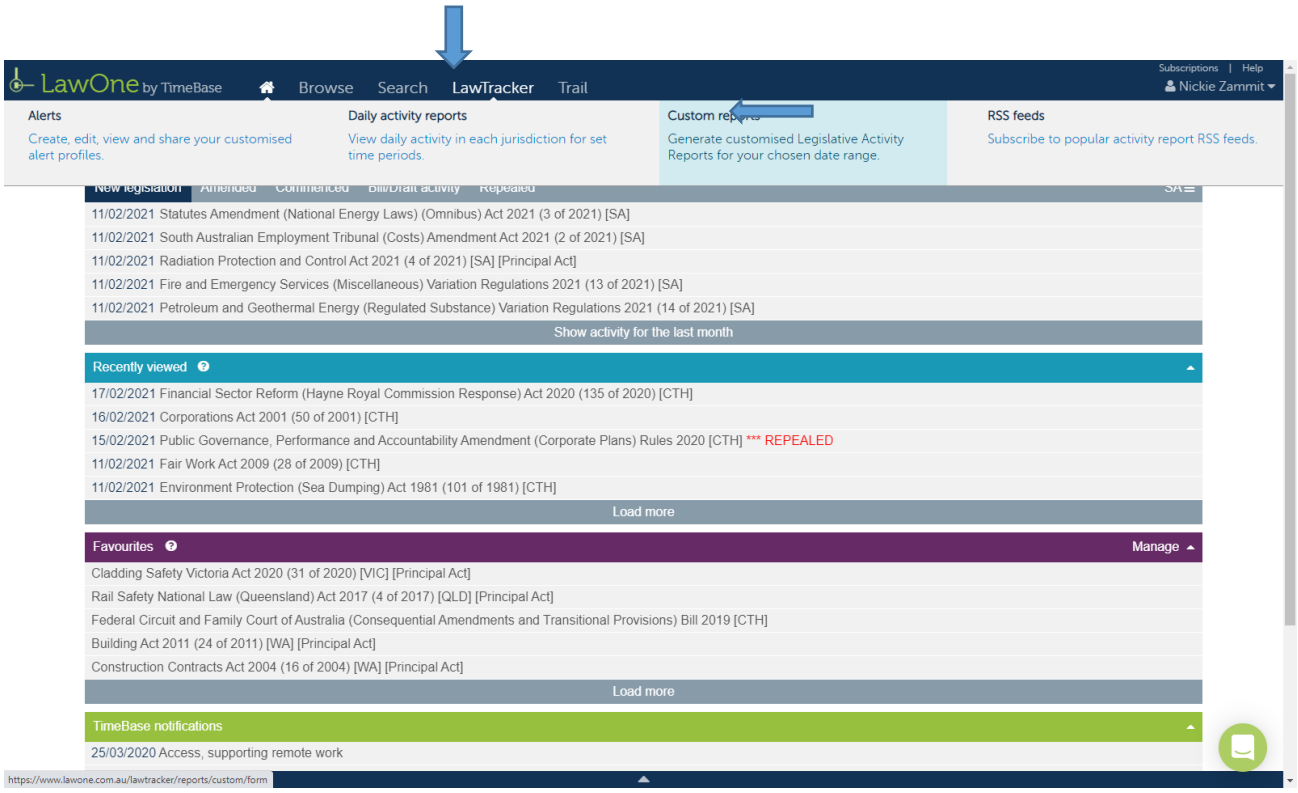




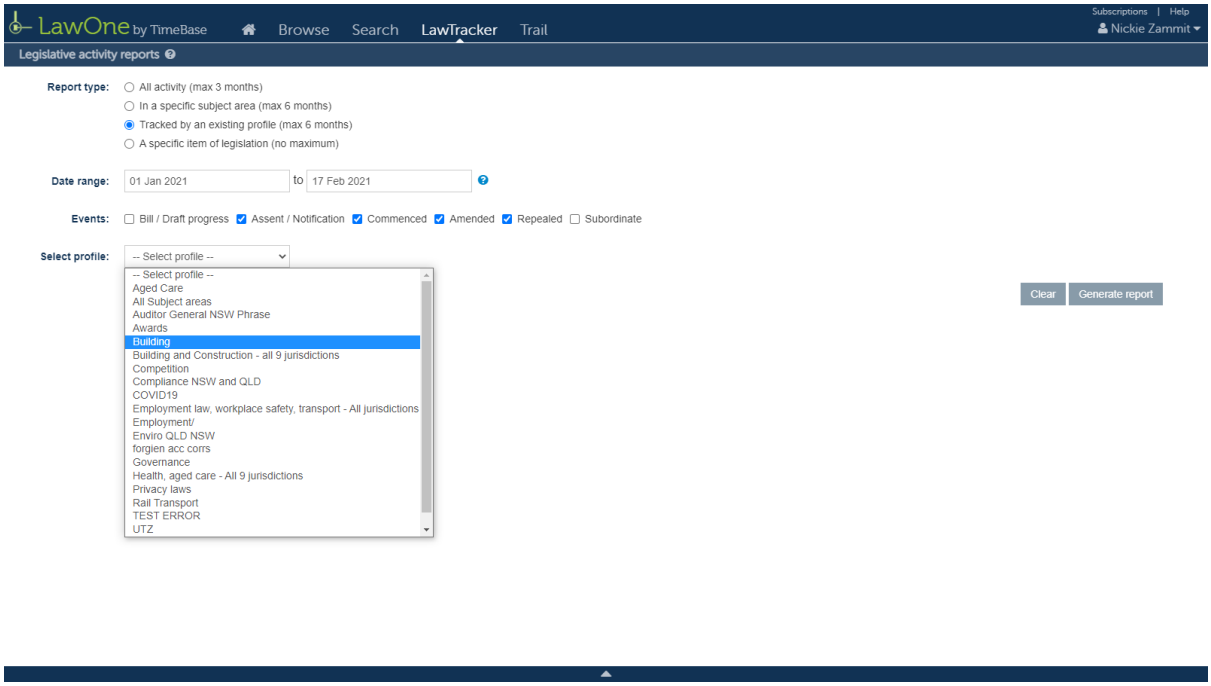
Running a Custom LawOne Report Instructions

To run custom reports on an Existing Profile

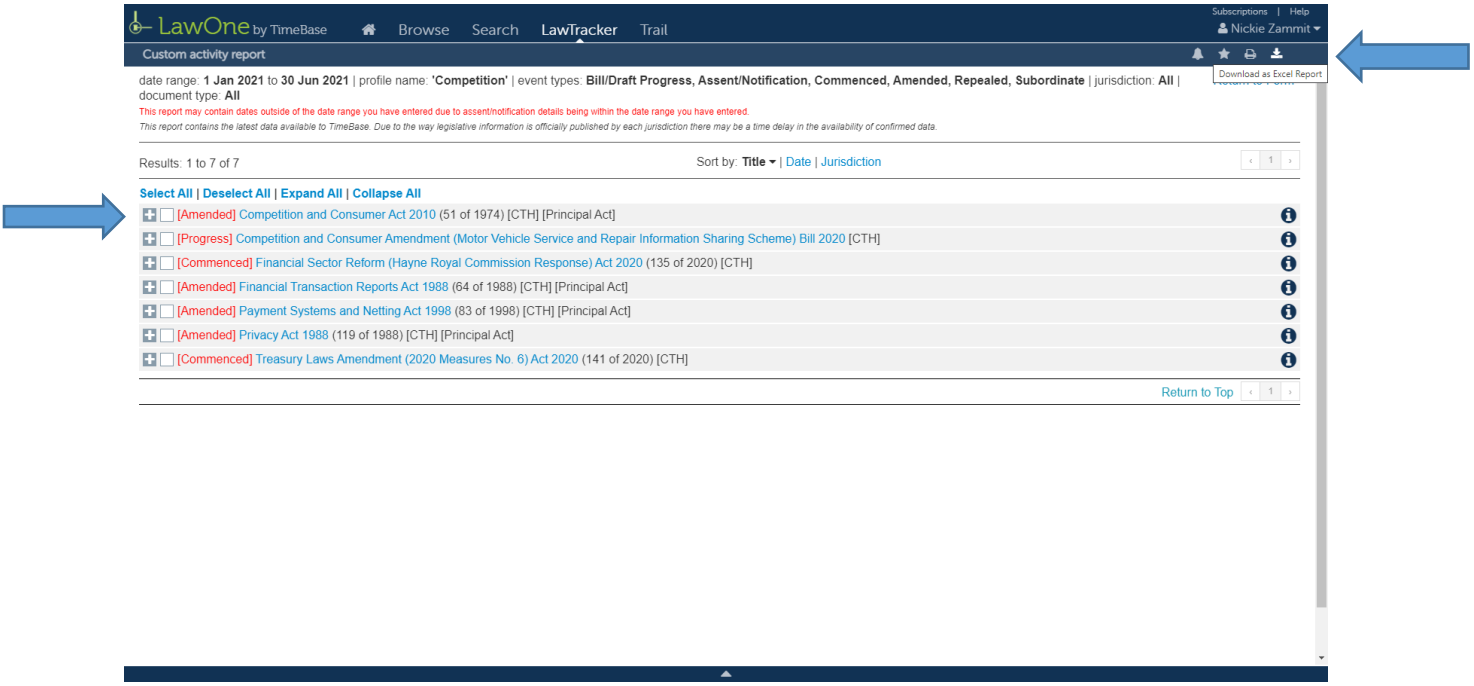
1. Login
2. Click on the “Lawtracker” tab
3. Then choose “Custom Reports”.



4. Tick the “Tracked by an existing profile”.
5. Enter in the date range.
6. Choose all the events you want to report on.
7. Select your profile from the drop-down box.
8. Click “Generate Report”.



9. The results will be displayed on your screen where you can click on the “+” signs to open up the details, or you can download the items in an Excel spreadsheet.



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

WESTERN SYDNEY
UNIVERSITY

COMPLIANCE INTERNAL CONTROLS
FACTSHEET

(Steps 5 and 7 of the Workflow)

WHAT ARE COMPLIANCE INTERNAL CONTROLS?

Internal controls are a consistent assurance of an organisation's objectives in complying with laws and regulations, mitigating any risk of non-compliance with an obligation.

WHAT ARE COMPLIANCE *KEY* INTERNAL CONTROLS?

Key Internal Controls have one or both of the following characteristics:

- Their failure could materially affect the compliance with an obligation.
- Their operation may prevent other internal control failures or detect such failures before they have an opportunity to become material to the organisation's objectives.

WHAT RISK IS THE COMPLIANCE CONTROL INTENDING TO MITIGATE?

The risk is non-compliance with a specific obligation on the University, as directed by a NSW or Cth statutory instrument.

WHO IS RESPONSIBLE FOR WRITING THE CONTROL DESCRIPTIONS?

The Nominated Compliance Contact assigned a law and obligation is responsible to write the control descriptions against the assigned obligation.

SHOULD I INCLUDE A CONTROL DESCRIPTION THAT IS NOT EXECUTED BY MY ROLE AND/OR OPERATING UNIT?

A key control should be executed and owned by the operating unit who is assigned a law. An assigned operating unit may list other internal controls executed by another business unit, which reduces the risk of non-compliance, but would not be considered a key control.

An operating unit should *certainly* list a control of another operating unit if they:

- Have oversight of that control/approves the execution of the control;
- Proactively trigger or directs the control execution in the other operating unit.

If there are any issues or questions, speak to the Compliance Program Unit, as assignment and accountability discussions may need to be had/escalated.

HOW MANY CONTROLS SHOULD BE LISTED PER OBLIGATION?

Generally, there should be only 1-3 controls per obligations, with 1 control being the key control.

HOW OFTEN SHOULD CONTROLS BE REVIEWED?

Controls should be maintained, reviewed *at least annually* (as Contacts attest to the controls' accuracy and currency in the annual attestation process), and tested (i.e. does the control do what it is intended to do, can it be bypassed, is it effective in reducing the impact or likelihood of non-compliance risk) to ensure their continuing effectiveness.

Controls should *always* reviewed in the event of strategic organisational restructure, when the control executor role has changed or no longer exists, or the obligation has been amended.

HOW SHOULD CONTROLS BE WRITTEN?

Control descriptions should be written to the following standard/guideline:

i) Include **who** owns and/or operates the control. *Use roles, not names.*

ii) Include the **frequency** of control operation. *Specify whether the control is executed daily, weekly, monthly, quarterly, annually, or as-needed (ad hoc).*

iii) Ensure there is an appropriate mix of **functions** and **practices** of controls.

- Functions include preventative (identify and address problems before they happen), detective (find incorrect, missing, or invalid items after they have occurred), and corrective controls. An optimal system of internal controls will a mixture of all three, but as a rule of thumb, there should be more preventative controls. Attached is the Compliance Controls Definition document, which has been operational since 2019.

- Practices include manual (human / judgment actions, such as approval), or automated controls (computerised/electronic actions).

iv) **Restate** the obligation to guide you in ensuring the control is a direct mitigant to the non-compliance risk.

v) Be in the **present tense** i.e. current. Is this control actively being executed, or is this outdated i.e. executed only in 2021

vi) Be a **factual** statement i.e. accurate. Is the control being executed as you state it is, or are you only executing a control annually but you have stated it is executed twice a year? *Do not write future controls not yet implemented Avoid intent/objectives by using the words "shall" or 'are required" as that does not make it factual.*

vii) Describe the control in **no more than a paragraph** being clear on the 'who', 'what', 'where', 'how', and possibly 'why'. i.e. Who is executing what activity when and where, and how are they doing it which can be used as evidence of the execution of the control.

- Training in and of itself is not an effective control. The tolerance for the training control is what drives its effectiveness. Specify what % of people must complete what task within what time period.

WESTERN SYDNEY
UNIVERSITY

EXAMPLES OF CONTROL DESCRIPTIONS

EXAMPLE 1

OBLIGATION

Sections 114-117 (Part 8 - Impounding of unattended and trespassing stock and abandoned articles)

The University must ensure that its livestock must not escape and be secured away from any public road or other public place.

CONTROL DESCRIPTION 1 (PHYSICAL SECURITY, preventative control measure)

Farm staff [*WHO*] prevent escape and secure livestock away from any public road or other public place by [*REWRITE THE OBLIGATION AS THE RISK OF NON-COMPLIANCE*]:

- adequately fencing with padlocks [*WHAT*] farm areas [*WHERE*] upon installation of the area and introduction of new livestock [*WHEN*];

- posting signs [*WHAT*] at all entry points [*WHERE*], advising visitors to contact the Farm Production Coordinator or Campus Safety and Security in the event of livestock escaping / on the road (the signs are installed at the time of an entry point is decided [*WHEN*]);

- transporting animals by truck [*WHAT*] across the major roads that separate farm paddocks (i.e. Blacktown Rd, Londonderry Rd and the River Farm) [*WHERE*] when livestock need to move paddocks [*WHEN*]

EVIDENCE OF CONTROL

SOPs, checklist, signed approval, consent form, logbook that states when gates/signs/padlocks/animals are installed/posted/checked/transported.

CONTROL DESCRIPTION 2 (ONGOING MONITORING, detective control measure)

Farm staff and Campus Safety and Security [*WHO*] detect whether livestock have escaped and are adequately secured from any public road or other public place by ensuring [*REWRITE THE OBLIGATION AS THE RISK OF NON-COMPLIANCE*]:

- checking all fence, gates and padlocks [*WHAT*] on each farm area [*WHERE*] each morning and night [*WHEN*] to ensure they remain unbroken and do not pose an escape risk.

EVIDENCE OF CONTROL

SOPs, checklist, signed approval, consent form, logbook that states when these checks are completed.

EVIDENCE OF COMPLIANCE WITH OBLIGATION

Locked gate and padlocked fences, no reports, or complaints of escaped livestock as evidence to the contrary.

EXAMPLE 2

OBLIGATION

Section 14 - Joint modern slavery statements (Part 2 - Modern slavery statements)

The University, as a reporting entity, must give the Minister a modern slavery statement for the entity, for a reporting period, which covers one or more reporting entities (which may include the entity giving the statement), for a reporting period for those reporting entities. The University must ensure that it:

(a) complies with section 16; and (b) is prepared in a form approved by the Minister; and

(c) is prepared in consultation with each reporting entity covered by the statement; and (d) is approved by the principal governing body (the Board of Trustees) of the University (the higher entity); and (e) is signed by a responsible member (the Vice-Chancellor) of the higher entity; and (f) is given to the Minister (uploaded to the Register) within 6 months after the end of the reporting period for the entities covered by the statement (June-end for calendar year reporting).

CONTROL DESCRIPTION 1 (CHECKLIST, preventative control measure)

The Director, Compliance [*WHO*] ensures the University's and Controlled Entities' Modern Slavery Statement for a reporting period is in consultation with all controlled entities, is approved by the Board of Trustees and signed by the Vice-Chancellor, and is uploaded to the Register by 30 June of the next year (subs c-f) by [*REWRITE THE OBLIGATION AS THE RISK OF NON-COMPLIANCE*]:

- adhering to the timeline, reminders, and checklist, and use of templates of board papers [*WHAT*] housed on its shared drives with Procurement [*WHERE*] between 1 January until 30 June of the following year [*WHEN*].

EVIDENCE OF CONTROL

The timeline/checklist and other documents, and emails.

CONTROL DESCRIPTION 2 (RECONCILIATION REPORTING, detective control measure)

The Director, Compliance [*WHO*] ensures the University's and Controlled Entities' Modern Slavery Statement for a reporting period is compliant with s 16, in the prescribed form (subs a-b) by [*REWRITE THE OBLIGATION AS THE RISK OF NON-COMPLIANCE*]:

- cross-referencing with s 16 of the current Modern Slavery Act 2018 (Cth) and other Regulator guidance

documents [*WHAT*] in regular meetings with Procurement [*WHERE*] from 1 November of the reporting period year until 1 March of the following year [*WHEN*]).

EVIDENCE OF CONTROL

Meeting invites and calendar reminders in Outlook, the cross-referencing with the legislation.

EVIDENCE OF COMPLIANCE WITH OBLIGATION

Signed Modern Slavery Statement uploaded to the Register.

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 Factsheet
- Self-Assessment Factsheet
- Legislative Alerts Factsheet
- Compliance Incident Reporting Factsheet
- Annual Attestation Factsheet

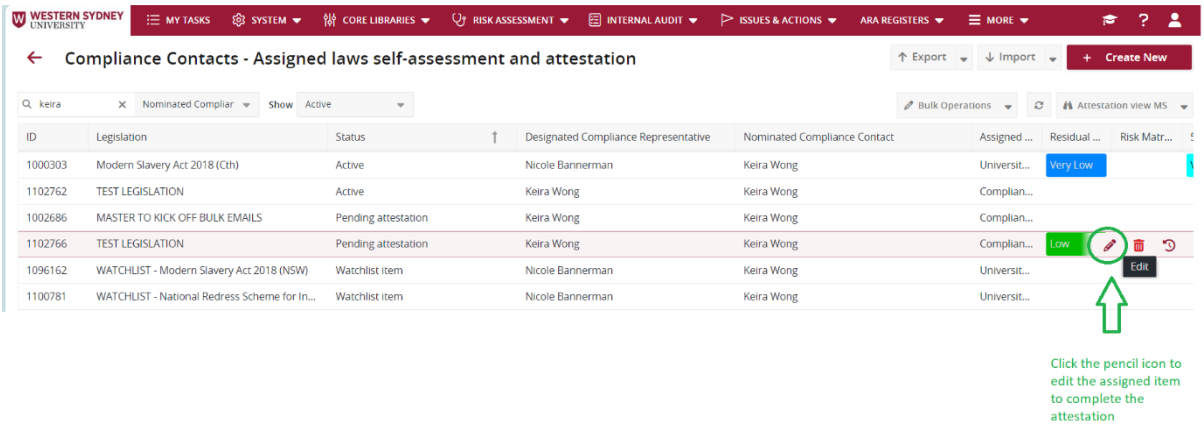
Self-Assessment Process Document for Step 5 of the Workflow

COMPLETE SELF-ASSESSMENT WITHIN 30 DAYS OF:

I) INITIAL ASSIGNMENT;
II) STRUCTURAL CHANGES; AND
III) REGULATORY AMENDMENTS.

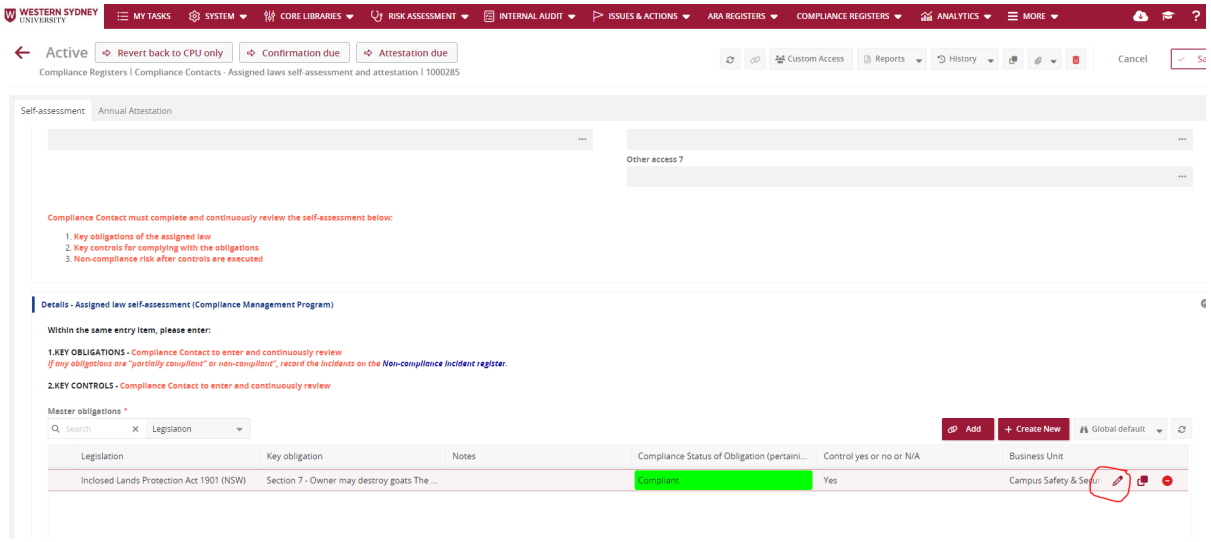
1. Access your Dashboard.

2. Click the pencil icon to update the assigned item.

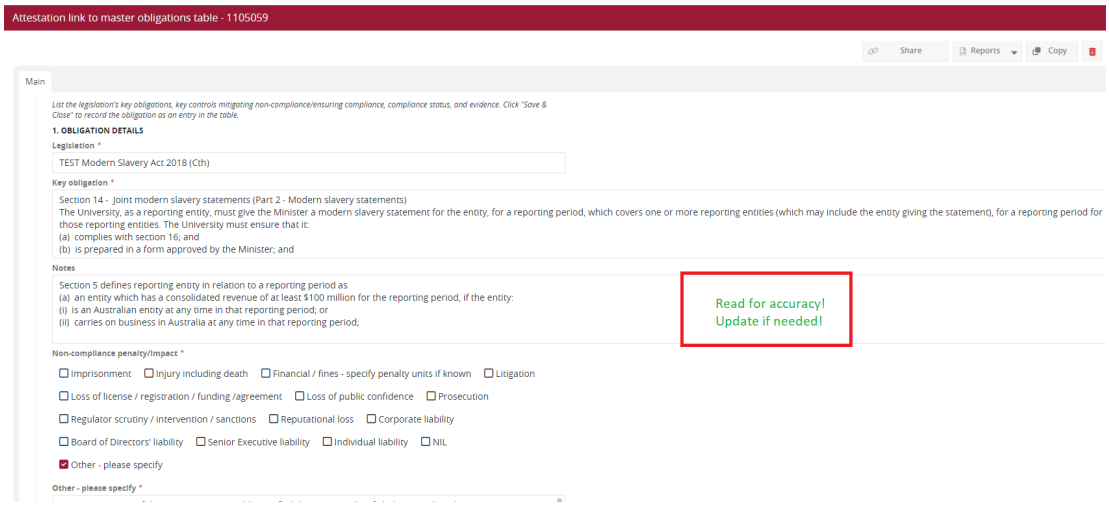


3. Scroll to the section labelled “Self-Assessment”.

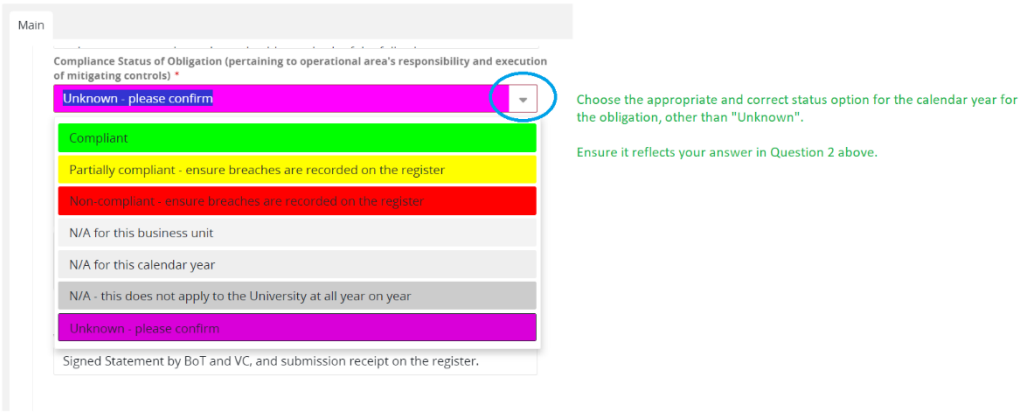
Double click the pencil icon on each obligation to update the following (opens up in new window)



Read and update the obligation (if needed).



Update the compliance status from “Unknown”



Note: If your obligations is ALREADY noted as “N/A for business unit” or “N/A for the calendar year” or “N/A for the University year on year” do not change it UNLESS it is inaccurate. You do NOT need to mark these as “Compliant”.

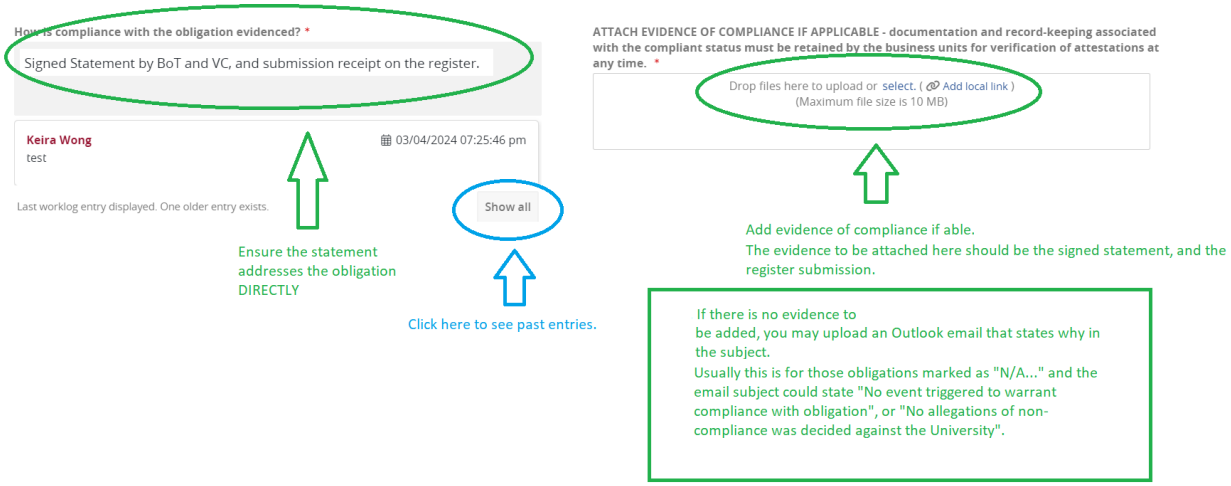
Update the statement of evidence of compliance (not needed if the status is marked “N/A...”)

This is a ‘worklog’ field, meaning it keeps an audit trail of previous entries. You will see a history of compliance statements from 2023 by clicking “Show all”.

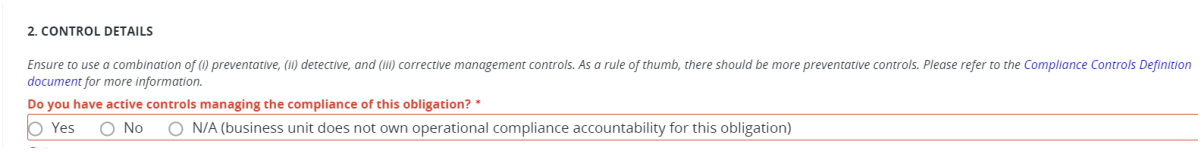
Update the attachment of evidence if able (not needed if the status is marked “N/A...”)

TIP: READ the obligation. The compliance must DIRECTLY address the obligation.

For example, it the obligation is to submit a report, then compliance is the report.
If the obligation is to NOT do an action, then compliance is the absence of it occurring, or the absence of any findings/decisions made against the University stating it has done the action.
If the obligation is to follow principles in activities, the compliance would be a strategic plan.

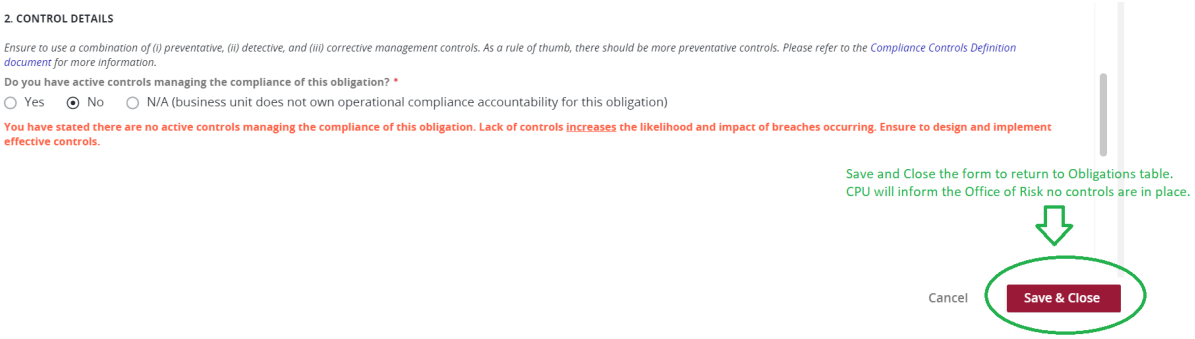


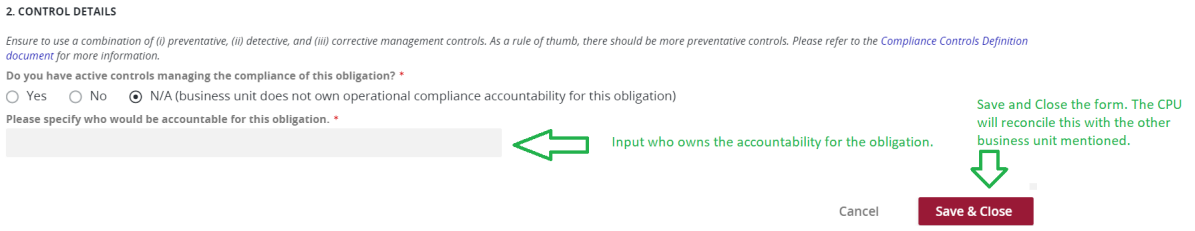
Update the controls that mitigate the non-compliance risk, adding more or deleting.



Answer “No” if there are no mitigating controls in place.
This may increase the risk of non-compliance with your assigned law.

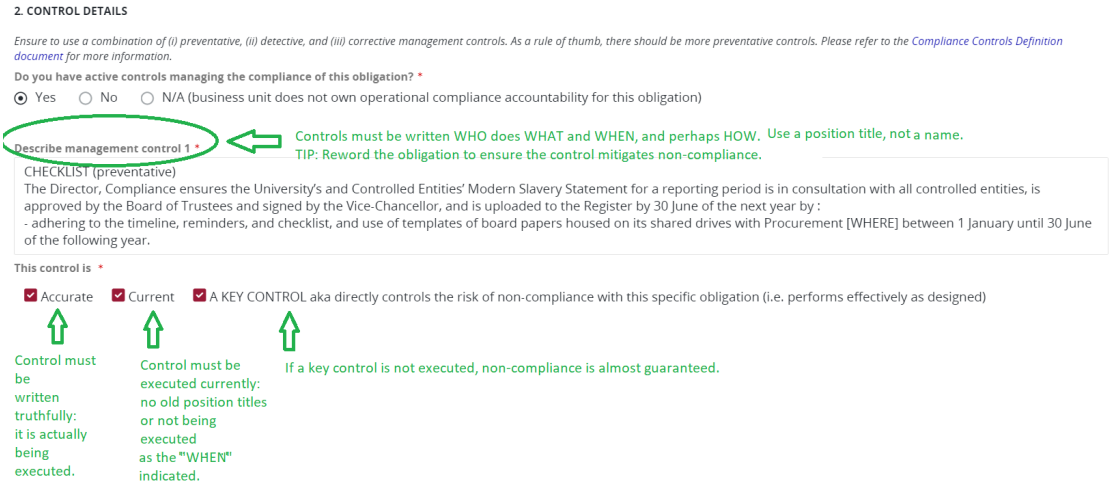
You will receive a warning notification and will be able to Save and Close the form to return to the Obligations table and repeat for any other obligations.





Answer “N/A” if the compliance status is “N/A for the business unit”.

You will need to state who owns the accountability in a new window.

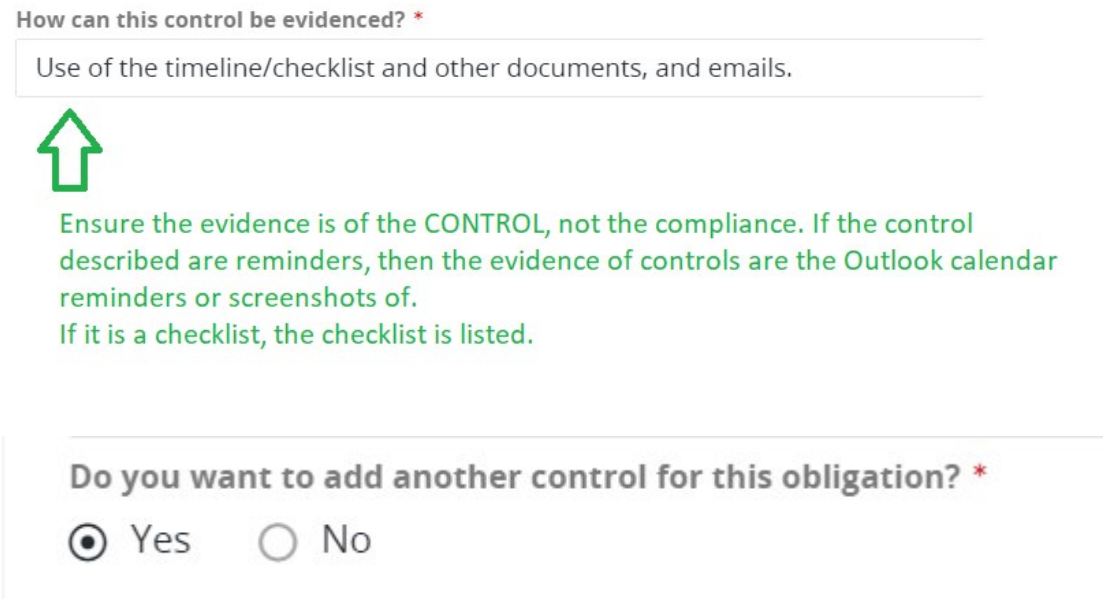


Answer “Yes” if you have mitigating controls in place to add (maximum of 5 to add – there should be some already listed with “Yes” already chosen).

Review the controls for accuracy and currency, update if needed.
The controls **must** be current and accurate (do not enter controls that aren’t yet executed)

There is a Controls Definitions Document linked to help.

Update the statement of evidence of controls

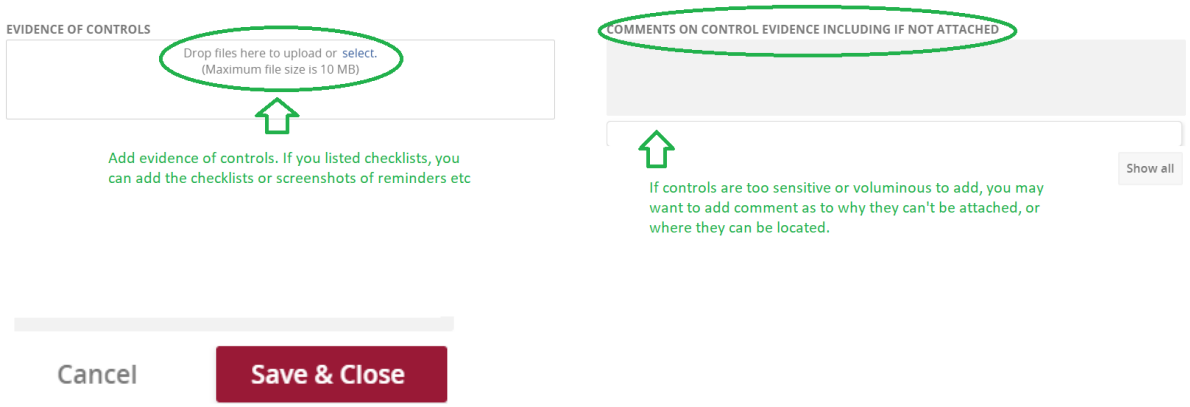


Answer “Yes” to add more controls (maximum of 5 can be added).

Answer “No” if there are no more controls to add.

TIP: There must be at least 1 key control listed, with a mixture of more preventative controls (use the help document) and some detective controls.

Update the attachment of evidence of controls, and comment



Click Save & Close to save the form and return to the obligation table.

REPEAT FOR ALL LISTED OBLIGATIONS IN THE TABLE.

Compliance Control Definitions

Preventative
Segregation of duties is the separation of duties to ensure the business complies with legislative obligations. For example, animals for research are being monitored by laboratory staff, as well as researchers, ensuring that the welfare of the animals are met.
Approval required - a process where an application for certain work to be done requires the signature of the manager/head of school.
Permission restrictions / data security - practices to keep information protected from, among other things, loss/corruption/unauthorised access/use. For example, requiring authentication for access or having data backed-up.
Delegation limits - a clear delegation framework to identify monetary limits, boundaries and accountability structures.
Automated workflow automates business processes**.** For example, if Condition A is met, then X will automatically occur. This (i) reduces the reliance on manual input and (ii) eliminates human error.
Identify /reference checks can be an internal control to manage risk in, for example, staff or student recruitment, or supplier engagement.
Checklist can be used as a reminder for staff to consider various factors in order to be compliant with legislative obligations.
Published standards or documented policies/ operating procedures to mitigate non-compliance of obligations. For example, by having standard operating procedures for staff to follow in respect of workplace safety.
Staff accreditation or professional training/ education includes any work induction a staff is required to complete prior to commencing work or on-going training to achieve compliance (i.e., maintain the required licences relevant to work).
Consent / ethics form are the required approvals to be obtained from relevant authorities prior to certain activities taking place.
Physical security includes keeping materials protected from unauthorised access/use. For example, securing hazardous materials in locked cabinets or setting up no-lone zones for when a particular activity occurs.

Detective
Exception / reconciliation reporting are reporting which flags discrepancies between actual and expected performances, used to highlight issues that require action. For example, account receivables and invoice reporting, inventory and expiration tracking for chemicals etc.

Detective
Ongoing monitoring is a process that ensures your area is kept informed of any changes or developments in compliance obligations that may impact business operations.
Management reporting includes a framework on how non-compliance of obligations can be identified, reported and managed. Consider whether your staff know of their compliance obligations and who they should report to. For example, by reporting to the Compliance Contact for the specific business unit if your staff are aware of a non-compliance risk.
Performance reviews include one-on-one meetings with staff members to discern their understanding of relevant legislative obligations pertaining to the University and the business unit, encouraging staff communication in reporting on non-compliance of obligations.
Investigations include processes and procedures (for example, through regular reviews and checks) to detect and monitor any non-compliance of obligations.

Corrective
Insurance plans transfer the risk to a third party, for example by purchasing fire insurance.
Business continuity plans is to have a well-defined strategy in place for when a breach of obligation that is likely to impact on the business' functions happens. Consider the level of resilience your business is in the event of a breach of obligation.
Crisis management plans are plans to handle non-compliance of obligations if it occurs. For example, a procedure that can restore a system if a launch fails.

Other
State other controls your business may have that is not already listed.

WESTERN SYDNEY UNIVERSITY

CONTINUOUS REVIEW & COMPLIANCE INCIDENT REPORTING FACTSHEET

(Step 6 of the Workflow)

WHAT IS CONTINUOUS REVIEW?

Compliance Contacts are **expected** to continuously review and update their assigned laws (key obligations and compliance status, internal controls, residual risk rating) when changes occur to the:

- assigned laws (usually contained within the email alerts – refer to the *Legislative Alerts Factsheet);*
- internal operations of the operating area; and
- organisational strategy and/or operations.

Compliance Contacts are **expected** to proactively self-report on any actual or potential breaches of their assigned, and any other, laws. This is known as Compliance Incident reporting.

WHAT IS A COMPLIANCE INCIDENT?

Compliance incidents are potential or actual occurrences that do not fulfil the University or its controlled entities' compliance requirements.

Incidents to report are non-compliance with legislative obligations, but also includes non-compliance with policy or procedure, as these incidents cause behaviours that do not conform to the compliance culture.

HOW TO REPORT COMPLIANCE INCIDENTS?

Report all incidences on the Compliance Incident Reporting Register.

Reports can be submitted by University or its controlled entities' staff other than designated Compliance Representatives and Compliance Contacts, or students, who have the option to submit reports anonymously.

WHY SHOULD I SUBMIT A COMPLIANCE INCIDENT REPORT?

Compliance incident reports should be submitted for a variety of reasons, including:

- ensuring a risk-based investigation and remediation of the incident is employed;
- preventing, minimising, and discovering similar incidents in other areas;
- disclosing the incident and steps taken for remediation for the purposes of management and Board Committee reporting; and
- demonstrating a genuine effort to report on and rectify an incident in a timely manner which may mitigate / reduce any future penalties that may be imposed.

WHAT HAPPENS WHEN I SUBMIT A COMPLIANCE INCIDENT REPORT?

All *referred* compliance incident reports (i.e. incidents *not* pertaining to the area of the individual reporting) are sent to the Compliance Program Unit ("CPU"). The CPU will ask additional information before referring to the operating are to whom the incident pertains in order to ascertain:

- Whether the incident is an isolated, deliberate, or systemic breach. This will inform the type of corrective actions to implement.
- Whether to refer the matter to, or work in consultation with, another managing department with specialised knowledge i.e. the Privacy Office, Work Health and Safety.
- The significance of the breach.

All *self-reported* compliance incidents are for the operating area to address and manage to resolution, which include:

- Any breach prevention plans and/or action for potential incidents.
- Root cause analysis of actual incidents, which will inform the type of corrective action to implement.
- Which corrective action/s were decided, and to follow up on the progress of the incident's remediation.
- Whether the incident should be escalated to Senior Executive Management and/or reported to the Audit and Risk Committee. All significant breaches are reported.

Root cause analysis includes finding out how the incident happened, why an incident happened, what triggered it, and ultimately ensuring it does not recur. It examines the controls in place, the behaviours and relationships of those involved, and what should have happened versus what did happen. Refer to the *Root Cause Analysis Guideline* accompanying this Factsheet.

IS THERE TRAINING?

Yes. Training on the Compliance Management Program, of which the Compliance Incident Reporting 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
- Self-Assessment Factsheet
- Annual Attestation Factsheet

WESTERN SYDNEY
UNIVERSITY

ROOT CAUSE ANALYSIS
5WHYS AND 6P METHODOLOGY
GUIDELINE

WHAT METHOD OF ROOT CAUSE ANALYSIS IS UTILISIED BY THE UNIVERSITY'S COMPLIANCE MANAGEMENT PROGRAM?

The Program utilises a combination of modified methodologies to best determine the root cause of a breach:

i) **Ishikawa**, an exercise to identify possible root cause(s) of an overall effect (the actual breach), coupled with the **6P matrix** (modified from the 8P, 4S, and 5M matrixes), a format to organise possible root cause(s) into the most common categories of root causes.
ii) **5 Whys**, an interrogative process to uncover what is the root cause(s).
iii) **GUT** prioritisation, a tool that determines in what order to resolve multiple root causes.

There are a handful of established techniques and methods for root cause analysis that are used for different industries from manufacturing to marketing. The Program uses the methodology most common in Lean Six Sigma, a process and performance improvement principle.

WHAT IS THE ISHIKAWA AND 6P MATRIX?

Ishikawa is traditionally a visual exercise to determine the possible categories of a problem. The 6P matrix are the 6 most common categories (all beginning with 'P', hence 6P) that can cause a breach:

i) Procedures - documented process, workflow, or procedures, can include policies.
ii) Platforms - digital platform or systems.
iii) Parts - machinery or equipment, physical items, maintenance.
iv) Place - environment (e.g. weather, natural disasters) or surroundings including locations.
v) Providers - third party suppliers.
vi) People - operational or functional labour of people, training, communication.

As the root cause analysis of a breach is conducted on the online Risk and Compliance system, the Program has modified this methodology by inverting the exercise (categories are asked last rather than first). The Program has also modified the 6P categories to best fit the higher education legislative context.

WHAT IS THE 5WHYS TECHNIQUE?

The 5Whys technique is applied to determine which of the 6 common and possible root causes is the actual root cause of a breach by asking for further explanation as to why (or most importantly *how*) something happened. It may uncover the possible cause category is the actual root cause, or it may uncover it was just a causal or contributory factor rather than a root cause, and it is, in fact, another category that was the actual root cause.

It is called the *5*Whys because the root cause is generally flushed out after asking for further explanation 5 times. It may be less, but generally it should be aimed to be answered in 5-7 steps. The University modified the 5Whys technique by preferring to ask '*how*' did something occur, as to '*why*' something occurred.

WHY SHOULD WE ASK 'HOW' INSTEAD OF 'WHY'?

When answering the "How" question, focus on answers based on facts, rather than assumptions, by which can be backed up by evidence, is measurable, and has the capability of being changed/altered i.e. what has actually happened, as opposed to guessing what might have happened. The "Why" question inevitably places blame on an individual, which is not the purpose of the RCA.

The philosophy behind the Ishikawa 6P methodology is people are less likely the root cause, as often the root cause was the process or environment in which the individual was working. Human error is often seen as an *effect*, rather than a cause, of systemic vulnerabilities deeper inside an organisation. Further, simply stating what people should have done doesn't explain why it made sense for them to do what they did in the first instance.

WHEN IS THE ROOT CAUSE FOUND IN THE 5WHY TECHNIQUE?

The root cause is discovered when the next 'how/why' is not useful/helpful in creating a solution i.e. changing / altering the error, or if it is beyond the organisation's control.

The "Why" also insinuates or compels a reason for intent or motivation, which cannot be measured, and would be based on an assumption. Intent and motivation behind human error may be absent altogether.

EXAMPLE 1 OF HOW TO FIND THE ROOT CAUSE USING THE 5WHYS

Breach: University-owned deer caused damage to a house and vehicle not owner by the University.

i) How did this occur? The deer escaped from the University paddock.
ii) How did this occur? The gate was open.
iii) How did this occur? The lock on the gate became unlocked.
iv) How did this occur? The lock was old and rusted.
v) How did this occur? The lock and gate were not maintained according to the recommended service schedule. **This is the root cause.**

6P category: Parts (maintenance).

Another root cause may be flushed out in one of the Why/How levels depending on the facts and context. You can track another path in the same 'interrogation' or start a new RCA using this new path.

EXAMPLE 2 OF HOW TO FIND THE ROOT CAUSE USING THE 5WHYS

Breach: University-owned deer caused damage to a house and vehicle not owner by the University.

i) How did this occur? The deer escaped from the University paddock.
ii) How did this occur? The gate was open.
iii) How did this occur? The lock on the gate became unlocked.
iv) How did this occur? The lock was not physically checked to see if it was still secure it was only visually checked from afar).
v) How did this occur? The procedure used by the safety officer did not direct to also physically check the lock. **This is the root cause.**

6P category: Procedure.

Another root cause may be flushed out in one of the Why/How levels. You can track another path in the same 'interrogation' or start a new RCA using this new path.

CAN THERE BE MORE THAN ONE ROOT CAUSE?

Yes, as seen with Example 2 above there is very often more than one root cause to a problem, which means there is more than one corrective action to implement.

A separate root cause does not necessarily need to have a separate 6P category. You can have two root causes categorised as 'Procedure', but they could be the overall procedure, and a checklist used by two different areas.

CAN I VERIFY THE ROOT CAUSE USING THE SAME TECHNIQUE?

Yes. Work backwards of the 5Whys process to verify if the interrogation progression follows a logical path. That means - read the explanations (the Hows/Whys) in reverse order. It should follow a logical progression to the breach. Using Example 1 above:

The lock was not maintained according to the maintenance schedule
(the root cause).
Therefore, the lock became old and rusted over time without anyone checking its quality.
Therefore, the deterioration caused the lock to become unlocked.
Therefore, the gate swung open.
Therefore, the deer escaped the paddock.
Therefore, the deer left the University campus and entered a neighbouring property, subsequently causing damage (the original breach statement).

A separate root cause does not necessarily need to have a separate 6P category. You can have two root causes categorised as 'Procedure', but they could be the overall procedure, and a checklist used by two different areas.

WHAT ARE CORRECTIVE ACTIONS?

Corrective actions resolve the identified root cause of the breach to prevent recurrence of multiple future breaches in the operating unit and perhaps other operating units.

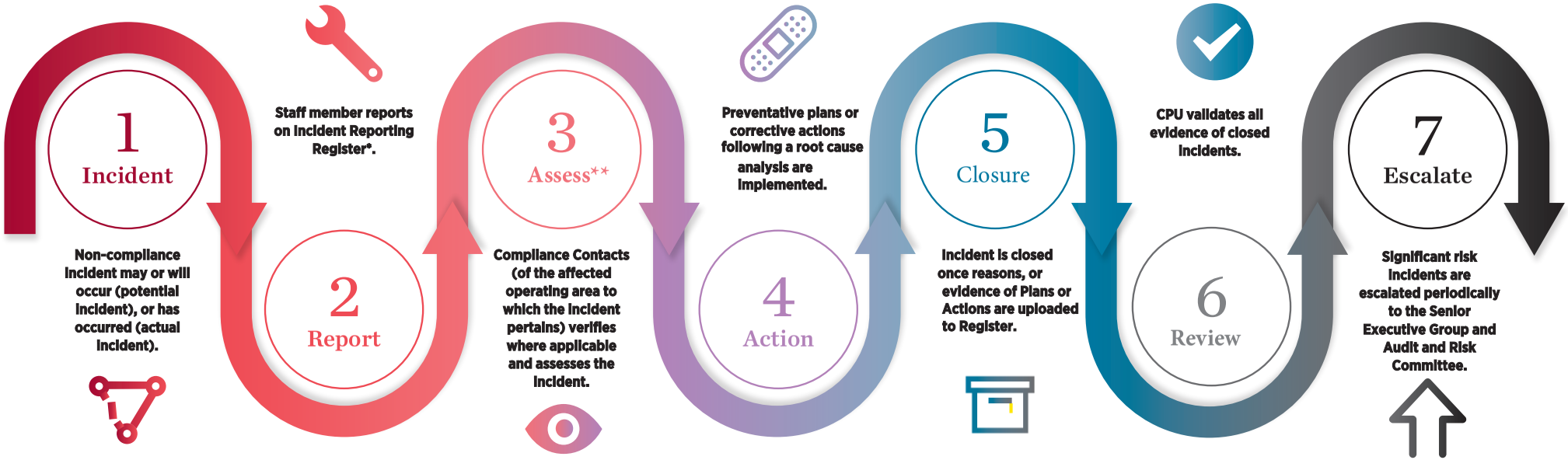
It is expected that i) updates to Procedures/Parts etc will take 3 months to implement; ii) creation of Procedures/Parts etc will take 6 months to implement; and iii) procurement of Systems etc will take 12 months to implement.

QUICK TIPS

- Pay attention to the logic of cause-and-effect relationship.
- Try to make answers more precise.
- Look for the cause step by step. Don't jump to conclusions.
- Base statements on facts and knowledge.
- Assess the process, not people.
- Never leave "human error", "worker's inattention", "blame John", etc. as the root cause.
- Make sure that root causes certainly led to the mistake by reversing the sentences created as a result of the analysis with the use of the expression "and therefore".

WESTERN SYDNEY
UNIVERSITY

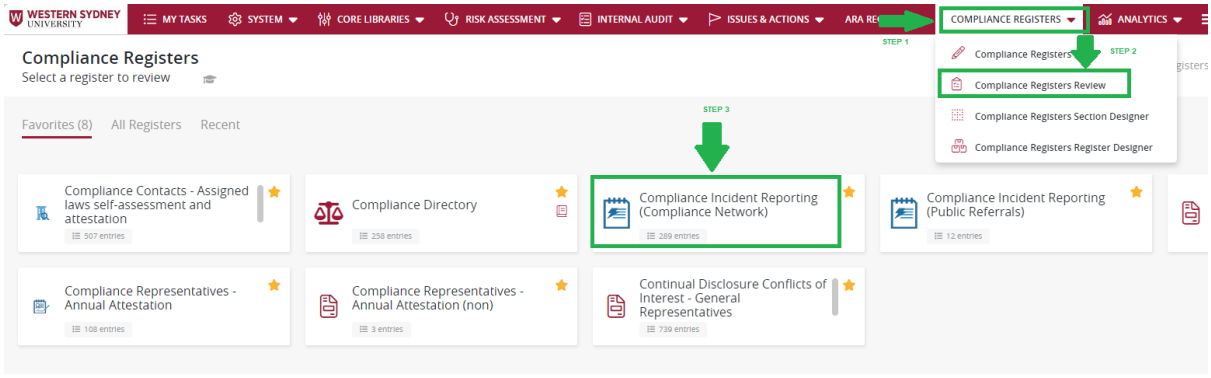
NON-COMPLIANCE INCIDENT REPORTING



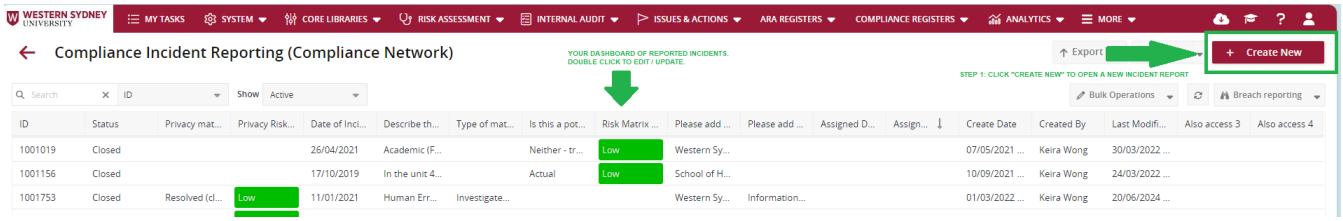
*Can self-report, and report anonymously (anonymous reports are first received by the Compliance Program Unit (CPU) for initial investigation to substantiate the report).
** If a referred incident is verified as unsubstantiated/without merit, incident may be closed with reasons as to why per Step 5 in the workflow.

Non-Compliance Incident Reporting Instructions for Step 6 of the Workflow

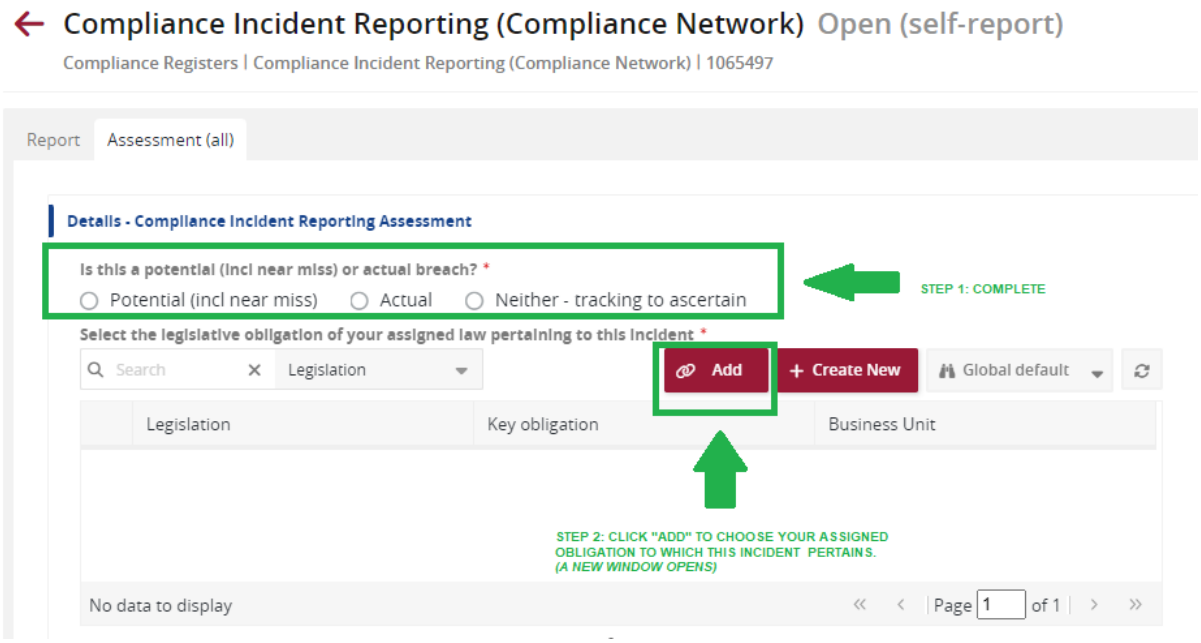
Log in to access the Reporting Register



Create New report from your dashboard



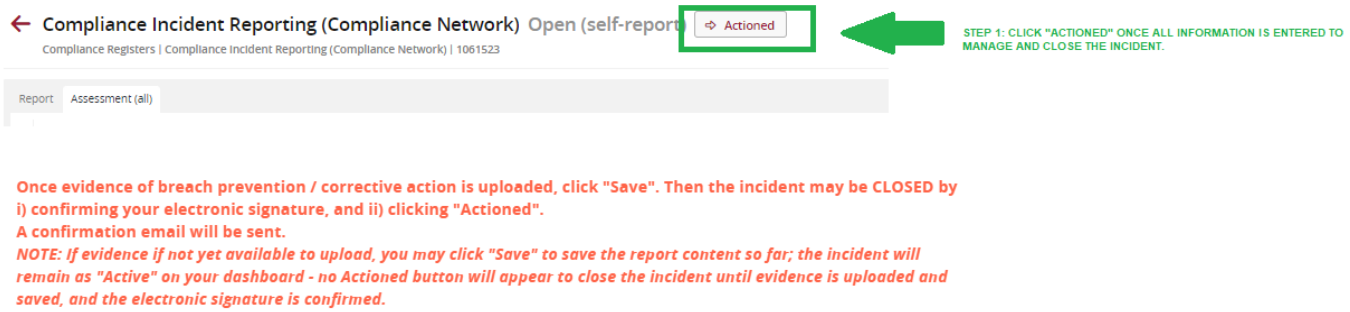
Complete all required details on the Report



Action the Report for submission once all required information is entered.

An incident will not be marked as closed unless confirmed as "Actioned". Reports are designed to stay open to ensure appropriate management.

Breach reporting tools are provided for use to ascertain root cause.



Once evidence of breach prevention / corrective action is uploaded, click "Save". Then the incident may be CLOSED by i) confirming your electronic signature, and ii) clicking "Actioned".
A confirmation email will be sent.
NOTE: If evidence if not yet available to upload, you may click "Save" to save the report content so far; the incident will remain as "Active" on your dashboard - no Actioned button will appear to close the incident until evidence is uploaded and saved, and the electronic signature is confirmed.

WESTERN SYDNEY
UNIVERSITY

ANNUAL ATTESTATION
FACTSHEET

(Steps 7-10 of the Workflow)

WHAT IS ANNUAL ATTESTATION?

Annual attestation assures the Board of Trustees, and any of its controlled entities' Boards, that there is no material non-compliance of the assigned laws in operating areas that could adversely affect the University or its controlled entities' ability to comply with legislative requirements.

Annual attestation is a *tiered approach*, where CCs attest first, followed by CRs based on CCs attestations, then finally DHs attest based on the two previous levels of attestations. The next level of attestation cannot complete their attestation until all of the previous level has attested. The CPU reports to the ARC on any delayed attestations.

Continuously reviewing the assigned laws, and timely reporting and management of compliance incidences, ensures a smooth attestation process.

WHO IS COLLECTING THE INFORMATION?

The University via the CPU is collecting the information regarding annual attestation.

WHAT IS THE PURPOSE OF THE COLLECTION?

The University is committed to good governance principles, and keeps a record of all its assurance activities, for audit and compliance purposes.

WHO HAS ACCESS TO THE INFORMATION IN THE ATTESTATIONS?

Attestations submitted by CCs, CRs, and DHs can be viewed and accessed by designated officers in the **Office of the University Secretary, and the Office of the University General Counsel** (i.e. Compliance Program Unit; Office of Audit and Risk).

It should be noted that external government authorities may request information about Attestations, especially in the event of a significant and/or reportable compliance incident.

ARE ATTESTATIONS ONLY KEPT ON UNIVERSITY SERVERS?

In some circumstances, Attestations may be entered on an online platform maintained by third party vendor, **Protecht**, which administers appropriate administrative, physical, technical safeguards and disaster recovery consistent with the requirements of ISO 27001 for the protection, security, confidentiality, and integrity of the data entered and stored in the Register.

Western Sydney University controls and limits access to the information in the Attestations. The University holds all data in its possession, and administers all data submitted and stored in accordance with its *Privacy Policy* and *Privacy Management Plan*.

Protecht does not (a) modify, (b) disclose except as compelled by law or as expressly permitted by Western Sydney University, or (c) access the data entered and stored in the Register except to provide maintenance services, prevent or address service or technical problems, or at Western Sydney University's request in connection with customer support matters.

HOW LONG WILL INFORMATION IN THE REGISTER BE STORED?

The information in the Register will remain in the Register until the agreement between the University and Protecht is

terminated (see next section).

WHEN WILL THE INFORMATION IN THE REGISTER BE DESTROYED?

Upon termination of the agreement the University has with Protecht, the data will be deleted within 30 days of the effective date of termination. A downloadable file of the stored data is made available to the University within the 30-day period. The data entered and stored in the Register will be cleansed from production and back up servers.

WHEN WILL WESTERN SYDNEY UNIVERSITY DESTROY THE INFORMATION PROVIDED FOR THE PURPOSE OF DECLARING CONFLICTS OF INTEREST?

Western Sydney University is bound by the *State Records Act 1998* (NSW), and retains Attestation records for 7 years. Note that using the online register does not absolve any retention requirements.

CAN I OPT OUT OF USING THE REGISTER?

Yes, you can opt out of having you're Attestation information entered and stored in the Register. This does not absolve the University requirement for compliance assurance, however, and a paper attestation must still be completed by you, and collected, used, and disclosed by the University in accordance with its *Privacy Policy* and *Privacy Management Plan*.

IS THERE TRAINING?

Yes. Training on the Compliance Management Program, of which the Annual Attestation 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
- Self-Assessment Factsheet
- Continuous Review & Compliance Incident Reporting Factsheet

Annual Attestation Instructions for Nominated Compliance Contacts

EMAIL SENT IN OCTOBER:

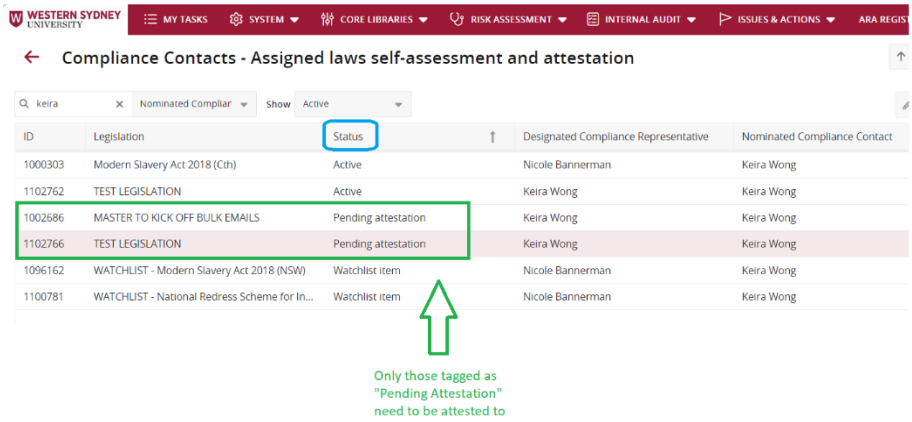
Compliance Program Unit (CPU) sends an email to the Nominated Compliance Contact with a link to the dashboard of all their assigned laws, instructing to complete the annual attestation for each assigned law.

COMPLETE ATTESTATION BETWEEN OCTOBER START TO NOVEMBER END

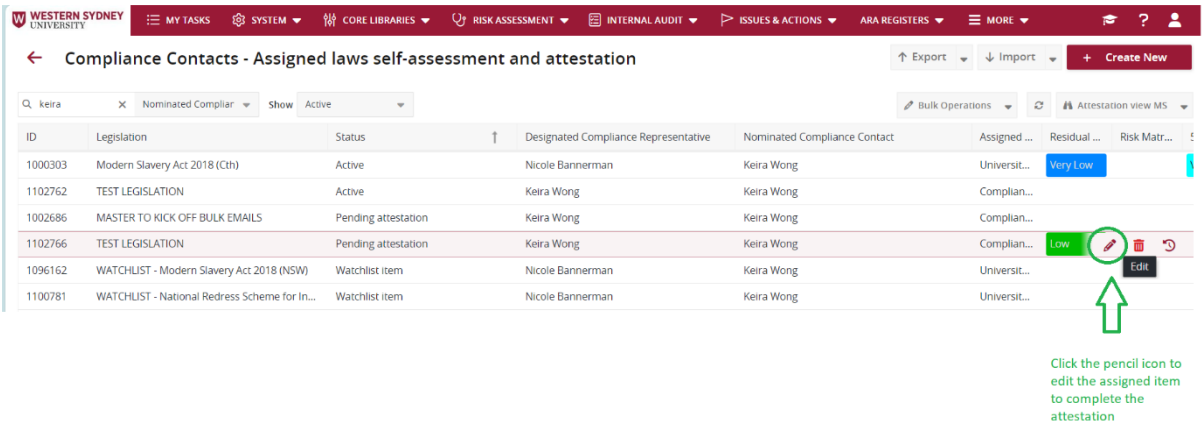
1. **Click the link provided.**

   The link will open to the dashboard of all assigned laws and Watchlist items.

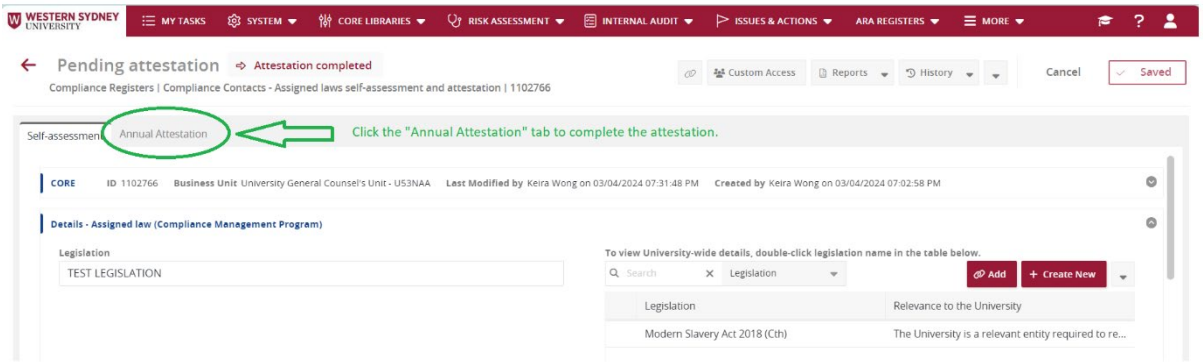
   Only assigned laws tagged as ‘Pending Attestation” in the status need to be annually attested to.



2. Click the pencil icon to update the assigned item.



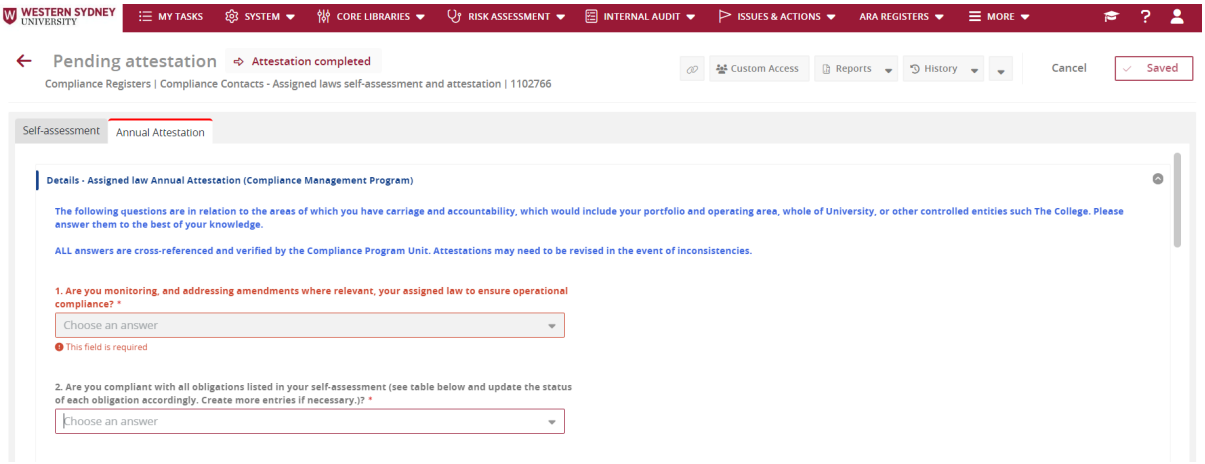
3. Toggle to “Annual Attestation” tab.



4. **Start answering the attestation questions.**

   They are all required to be answered and you will not be able to submit (or save) the form unless you complete all fields.

   TIP: If you need to Save the form to complete later, input 'dummy' text in the fields, and ensure the answers are changed to be accurate before submission.

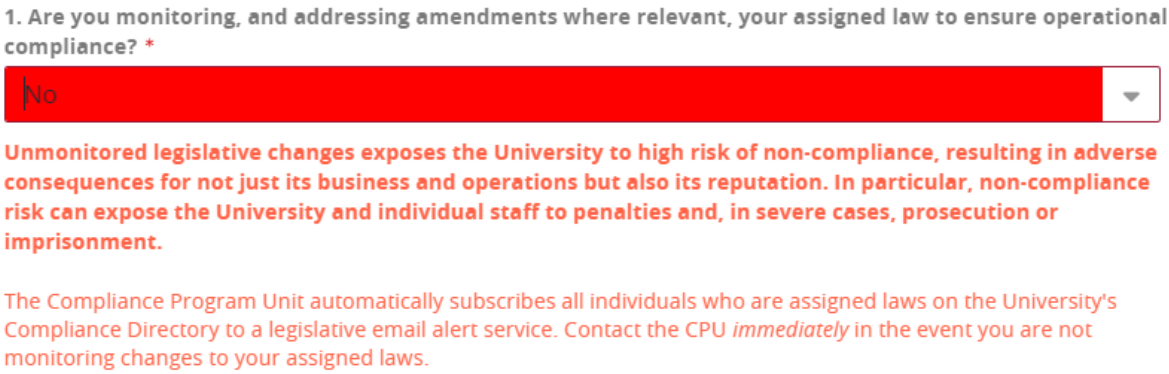


Here is a guide to the questions:

Question 1.

- Answer “Yes” if you are reading and addressing updates to your laws by subscribing to feeds etc (these, at a minimum, are the legislative email alerts from “LawOne@timebase”).

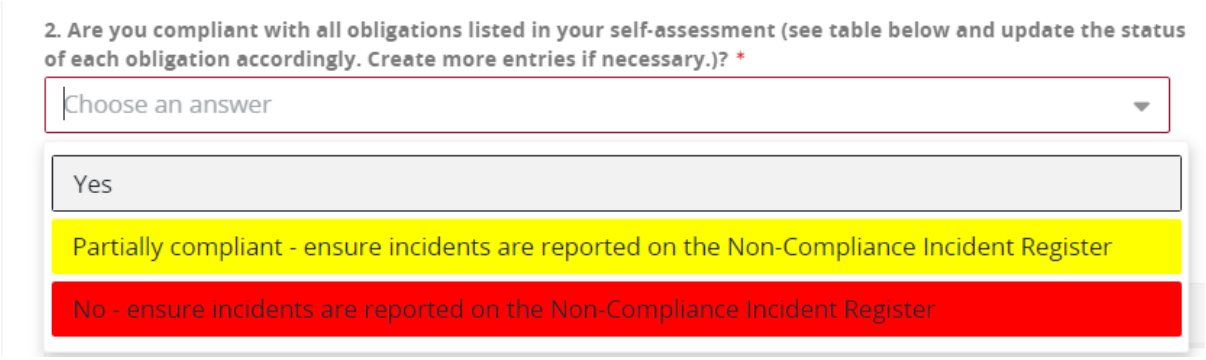
- Answer “No” if you are not monitoring your laws.
  This may increase the risk of non-compliance with your assigned law.
  You will receive a warning notification but will be able to proceed with the form.



Question 2.

This questions changes year on year to capture relevant Controlled Entity related questions on operations and custodianship.

Question 3.



- Answer "Yes" if you are compliant (i.e. no breaches or near-misses in the calendar year to *any* of your obligations.)

- Answer "Partially compliant" if there have been breaches or near-misses to some but not all of your obligations. This may increase the risk of non-compliance with your assigned law.
  You will receive a notification and link to record any incidents on the non-compliance register, if you haven't already. You will be able to proceed with the form.

  ***Please record non-compliance with obligations on the Non-Compliance Incident Reporting Register.**

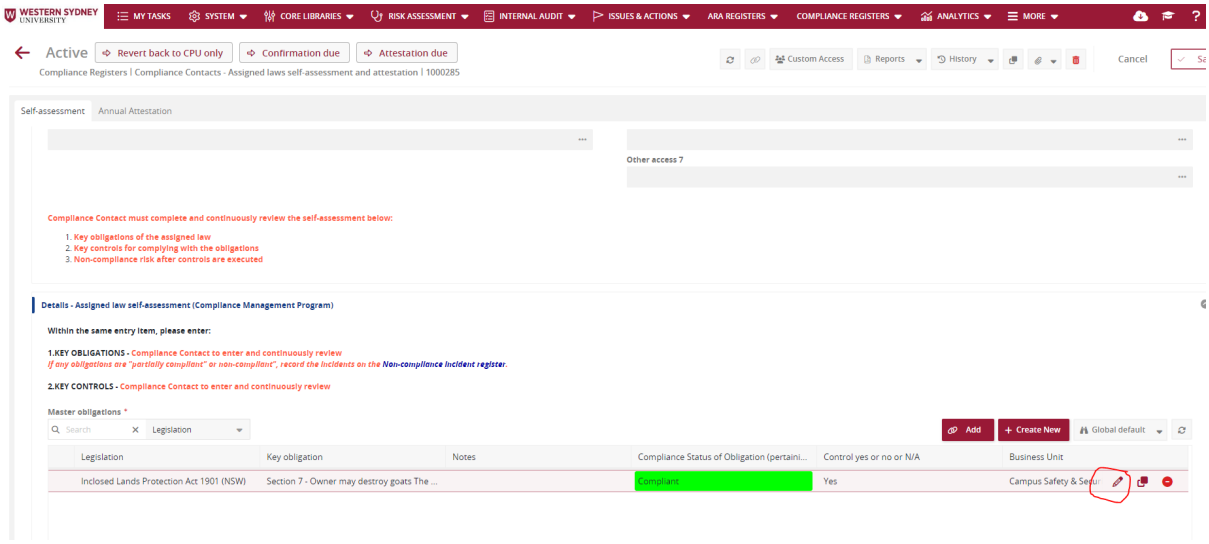
- Answer "No" if there have been breaches or near-misses to all of your obligations. This may increase the risk of non-compliance with your assigned law.
  You will receive a notification and link to record any incidents on the non-compliance register, if you haven't already. You will be able to proceed with the form.

***Please record non-compliance with obligations on the Non-Compliance Incident Reporting Register.**

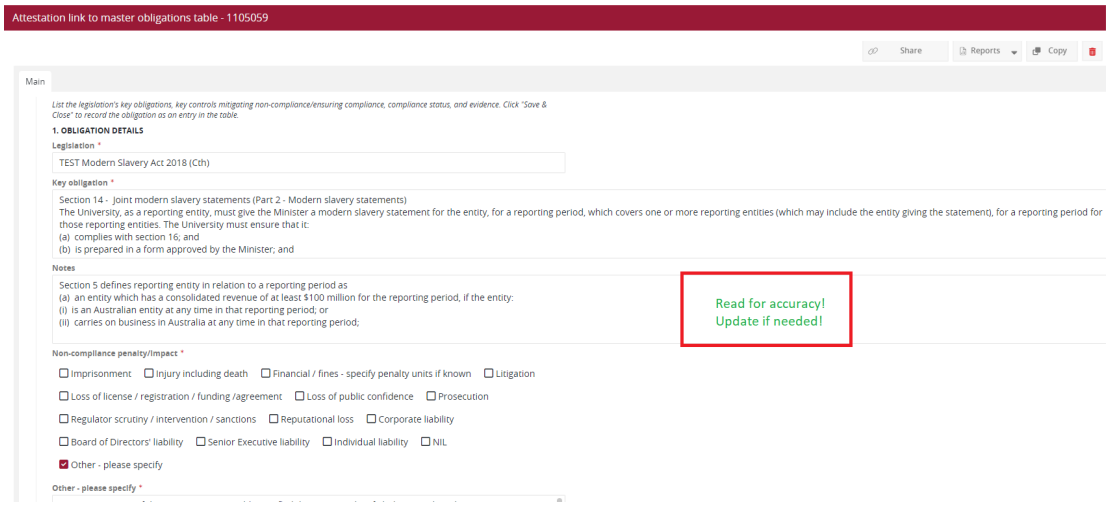
Note: Obligations noted as "N/A for business unit" or "N/A for the calendar year" or "N/A for the University year on year" will be taken as "Compliant".

Question 3A.

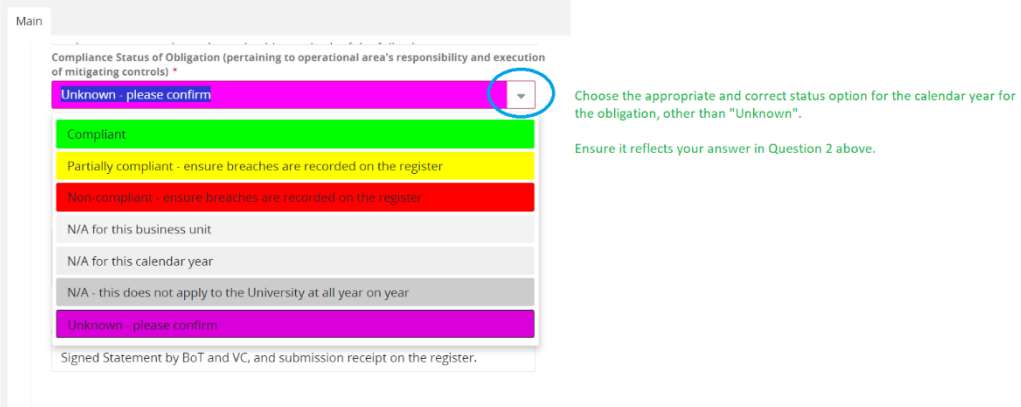
Double click the pencil icon on each obligation to update the following (opens up in new window)



Read and update the obligation (if needed).



Update the compliance status from “Unknown”



Note: If your obligations is ALREADY noted as “N/A for business unit” or “N/A for the calendar year” or “N/A for the University year on year” do not change it UNLESS it is inaccurate. You do NOT need to mark these as “Compliant”.

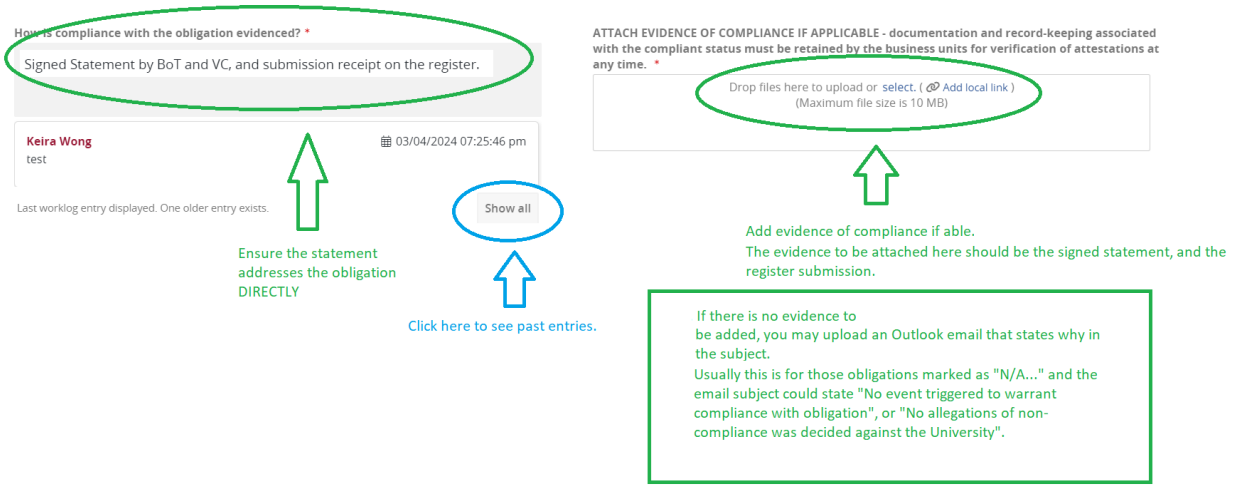
Update the statement of evidence of compliance (not needed if the status is marked “N/A...”)

This is a ‘worklog’ field, meaning it keeps an audit trail of previous entries. You will see a history of compliance statements from 2023 by clicking “Show all”.

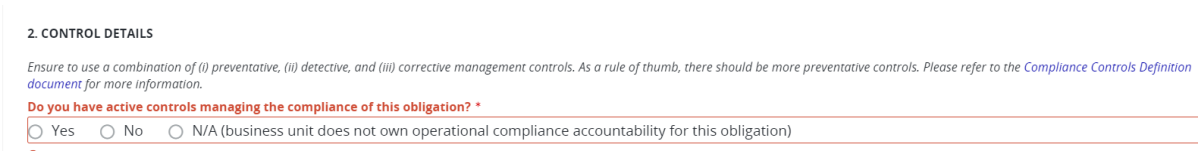
Update the attachment of evidence if able (not needed if the status is marked “N/A...”)

TIP: READ the obligation. The compliance must DIRECTLY address the obligation.

For example, it the obligation is to submit a report, then compliance is the report.
If the obligation is to NOT do an action, then compliance is the absence of it occurring, or the absence of any findings/decisions made against the University stating it has done the action.
If the obligation is to follow principles in activities, the compliance would be a strategic plan.

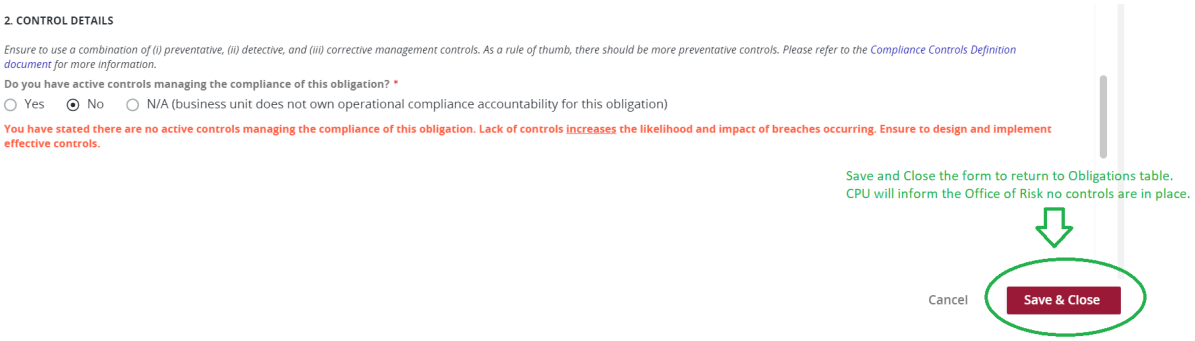


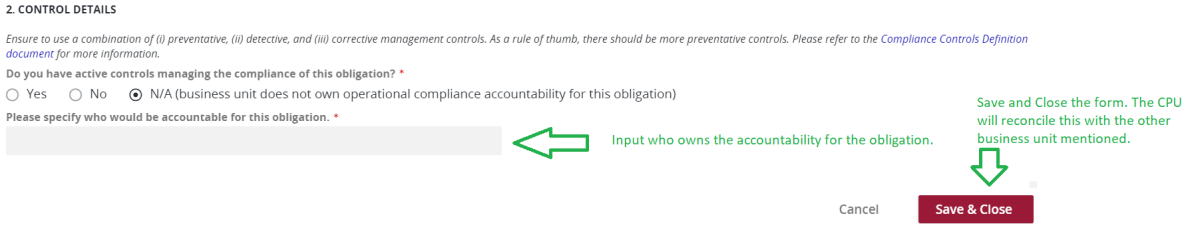
Update the controls that mitigate the non-compliance risk, adding more or deleting.



Answer “No” if there are no mitigating controls in place.
This may increase the risk of non-compliance with your assigned law.

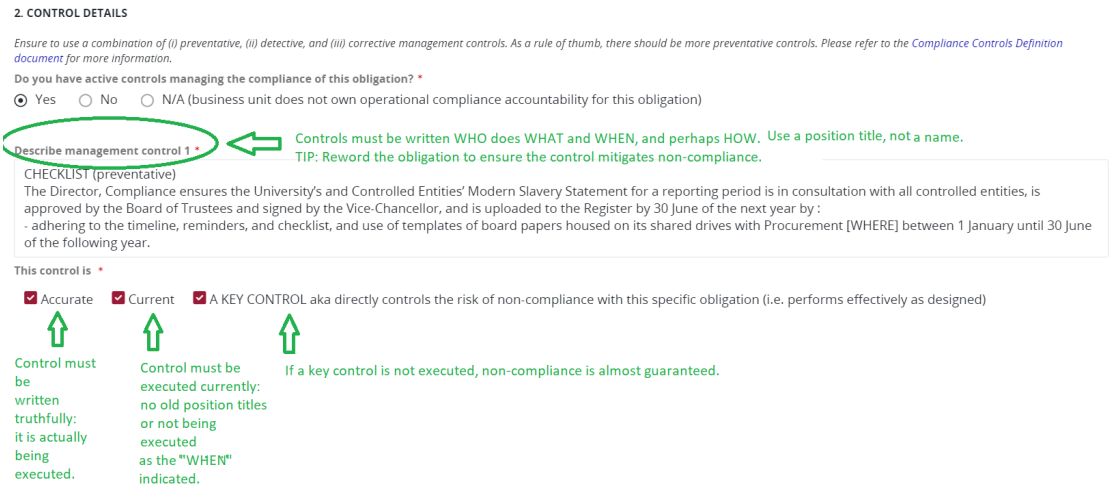
You will receive a warning notification and will be able to Save and Close the form to return to the Obligations table and repeat for any other obligations.





Answer “N/A” if the compliance status is “N/A for the business unit”.

You will need to state who owns the accountability in a new window.

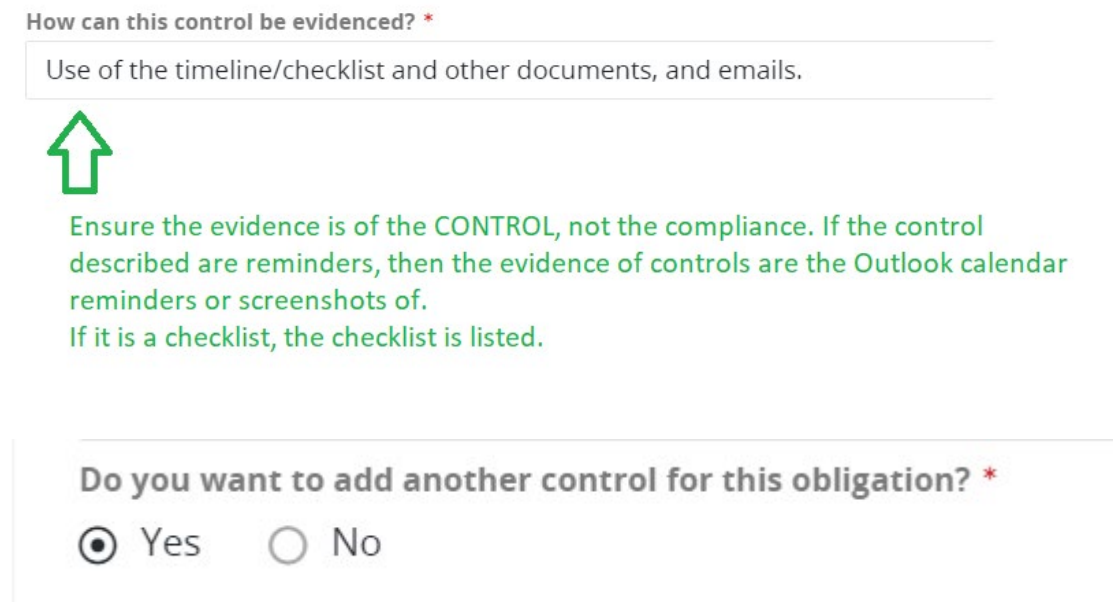


Answer “Yes” if you have mitigating controls in place to add (maximum of 5 to add – there should be some already listed with “Yes” already chosen).

Review the controls for accuracy and currency, update if needed.
The controls **must** be current and accurate (do not enter controls that aren’t yet executed)

There is a Controls Definitions Document linked to help.

Update the statement of evidence of controls

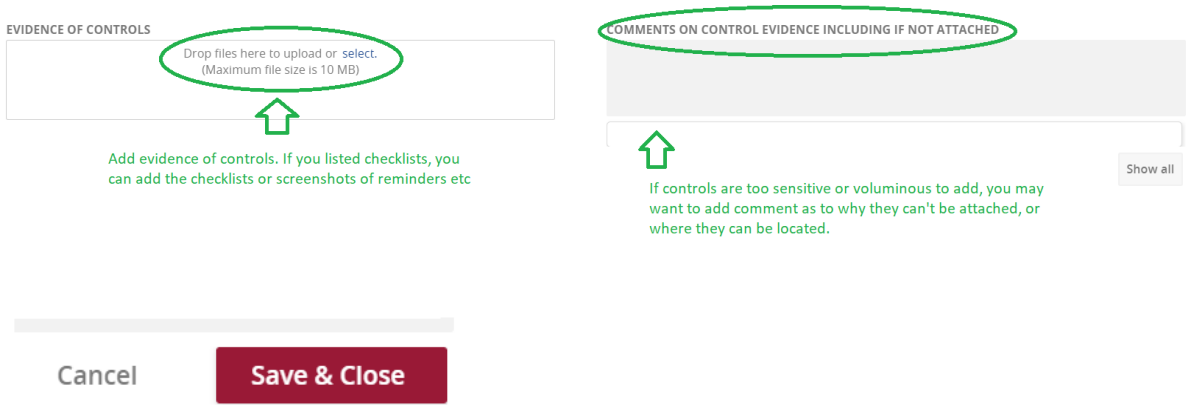


Answer “Yes” to add more controls (maximum of 5 can be added).

Answer “No” if there are no more controls to add.

TIP: There must be at least 1 key control listed, with a mixture of more preventative controls (use the help document) and some detective controls.

Update the attachment of evidence of controls, and comment



Click Save & Close to save the form and return to the obligation table.

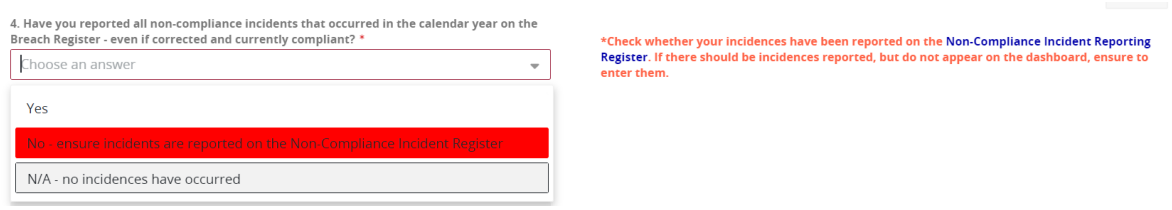
REPEAT FOR ALL LISTED OBLIGATIONS IN THE TABLE.

Question 4.

- Answer “Yes” if you uploaded evidence within the obligation
- Answer “No” if you did not upload evidence within the obligation.
- Comment on the evidence, such as location if not uploaded or ‘already attached in the obligation’.

Note: This may sound a bit repetitive but it is to ensure evidence is uploaded within the obligation which is usually missed.

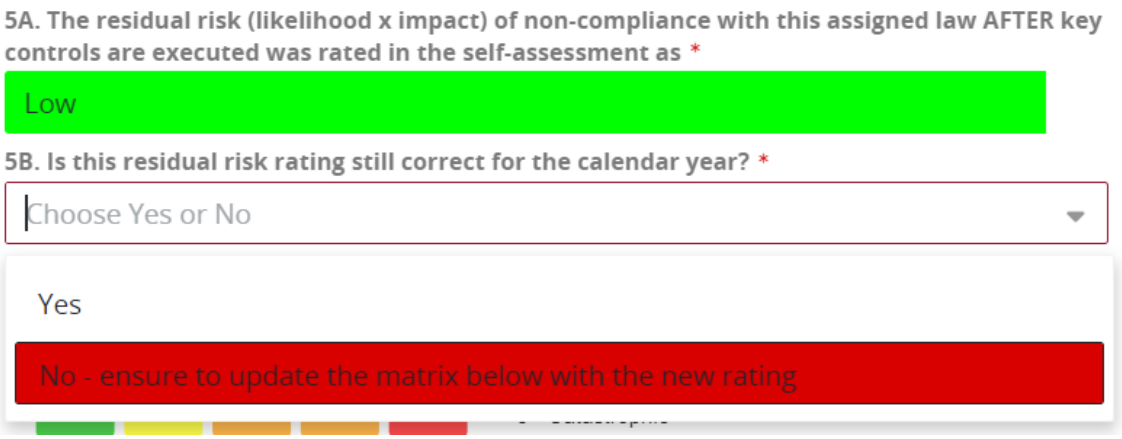
Question 5.



- Answer “Yes” if you have reported incidents throughout the year / before this part of the attestation ie when it was answered in the obligation.
- Answer “No” if you did not report incidents throughout the year / before this part of the attestation ie when it was answered in the obligation.
- Answer “N/A – no incidences have occurred” if there were NO breaches or near misses pertaining to any of your obligations throughout the year.

Note: This may sound a bit repetitive but it is to ensure incidents are reported for the law which is usually missed or forgotten.

Question 6.

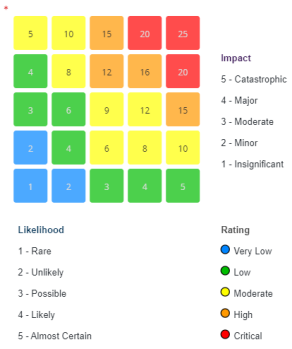


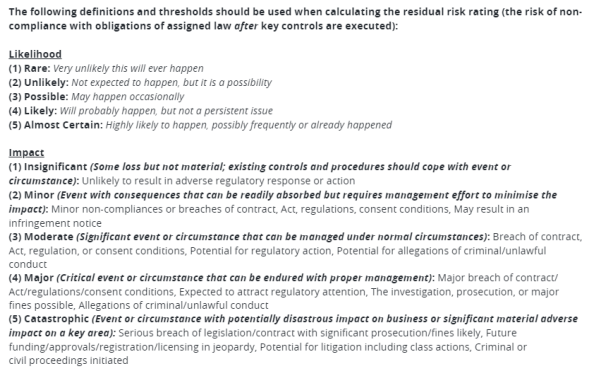
- Answer "Yes" if this residual risk rating of non-compliance still remains the same as listed.

- Answer "No" if the residual risk rating of non-compliance has *changed*.
    - This is usually because breaches have occurred (risk increasing), or controls are not accurate or current (risk increasing), or controls have gotten stronger ie another key control, more controls, better designed and / or operating controls (risk decreasing).

Question 6A.

The risk matrix will then become *required* for you to assess the residual risk again using the definitions on-screen for Likelihood and Impact.



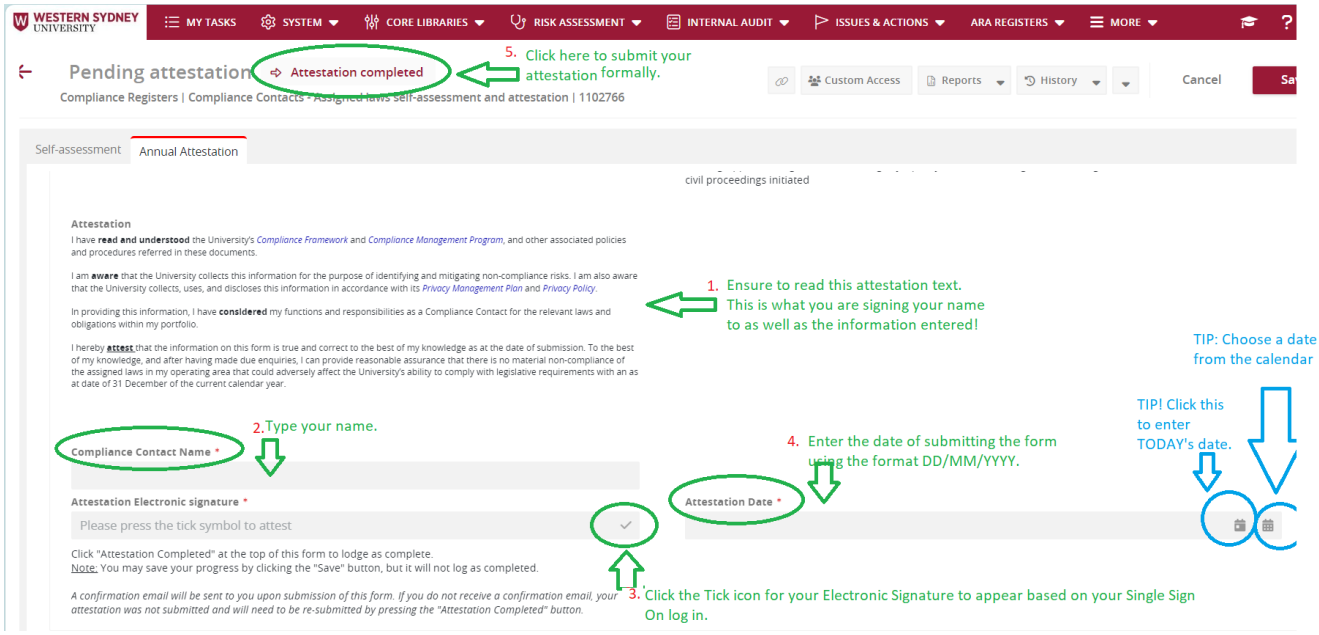


The following definitions and thresholds should be used when calculating the residual risk rating (the risk of non-compliance with obligations of assigned law *after* key controls are executed):

Likelihood
(1) Rare: *Very unlikely this will ever happen*
(2) Unlikely: *Not expected to happen, but it is a possibility*
(3) Possible: *May happen occasionally*
(4) Likely: *Will probably happen, but not a persistent issue*
(5) Almost Certain: *Highly likely to happen, possibly frequently or already happened*

Impact
(1) Insignificant ***(Some loss but not material; existing controls and procedures should cope with event or circumstance):*** Unlikely to result in adverse regulatory response or action
(2) Minor ***(Event with consequences that can be readily absorbed but requires management effort to minimise the impact):*** Minor non-compliances or breaches of contract, Act, regulations, consent conditions, May result in an infringement notice
(3) Moderate ***(Significant event or circumstance that can be managed under normal circumstances):*** Breach of contract, Act, regulation, or consent conditions, Potential for regulatory action, Potential for allegations of criminal/unlawful conduct
(4) Major ***(Critical event or circumstance that can be endured with proper management):*** Major breach of contract/ Act/regulations/consent conditions, Expected to attract regulatory attention, The investigation, prosecution, or major fines possible, Allegations of criminal/unlawful conduct
(5) Catastrophic ***(Event or circumstance with potentially disastrous impact on business or significant material adverse impact on a key area):*** Serious breach of legislation/contract with significant prosecution/fines likely, Future funding/approvals/registration/licensing in jeopardy, Potential for litigation including class actions, Criminal or civil proceedings initiated

5. COMPLETE AND SUBMIT YOUR ATTESTATION



1. Read the attestation text.
2. Type your name.
3. Click the Tick icon for your electronic signature.
4. Choose date for the lodgement of your attestation.
5. **Click the "Attestation Button" to submit your attestation formally.**

Annual Attestation Instructions for Designated Compliance Representatives for Step 9 of the Workflow