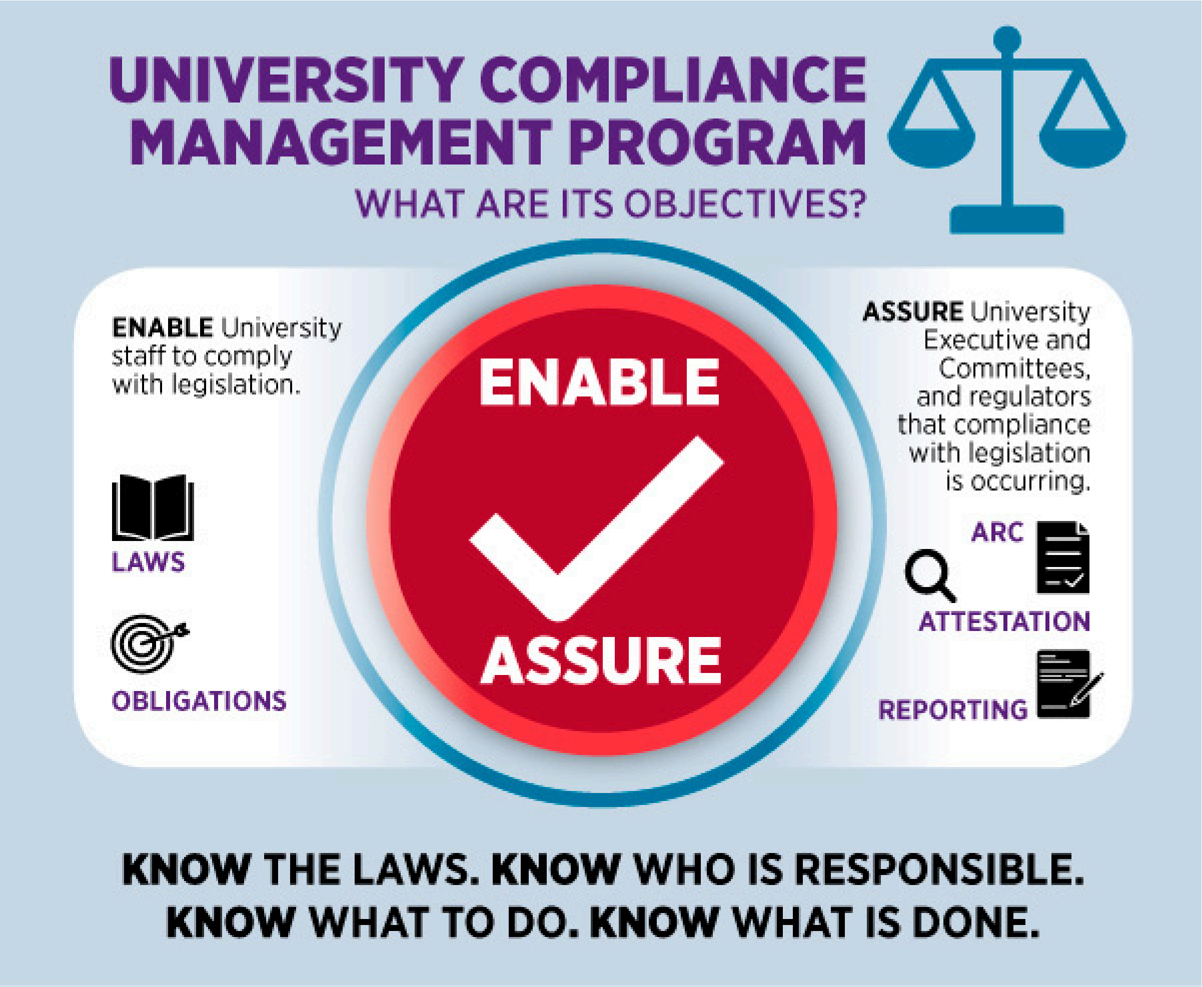
WESTERN SYDNEY
UNIVERSITY



UNIVERSITY COMPLIANCE MANAGEMENT PROGRAM

WHAT ARE ITS OBJECTIVES?

ENABLE University staff to comply with legislation.

LAWS

OBLIGATIONS

ENABLE

ASSURE

ASSURE University Executive and Committees, and regulators that compliance with legislation is occurring.

ARC

ATTESTATION

REPORTING

KNOW THE LAWS. KNOW WHO IS RESPONSIBLE. KNOW WHAT TO DO. KNOW WHAT IS DONE.

HOW TO

MANUAL

TO BE USED BY:

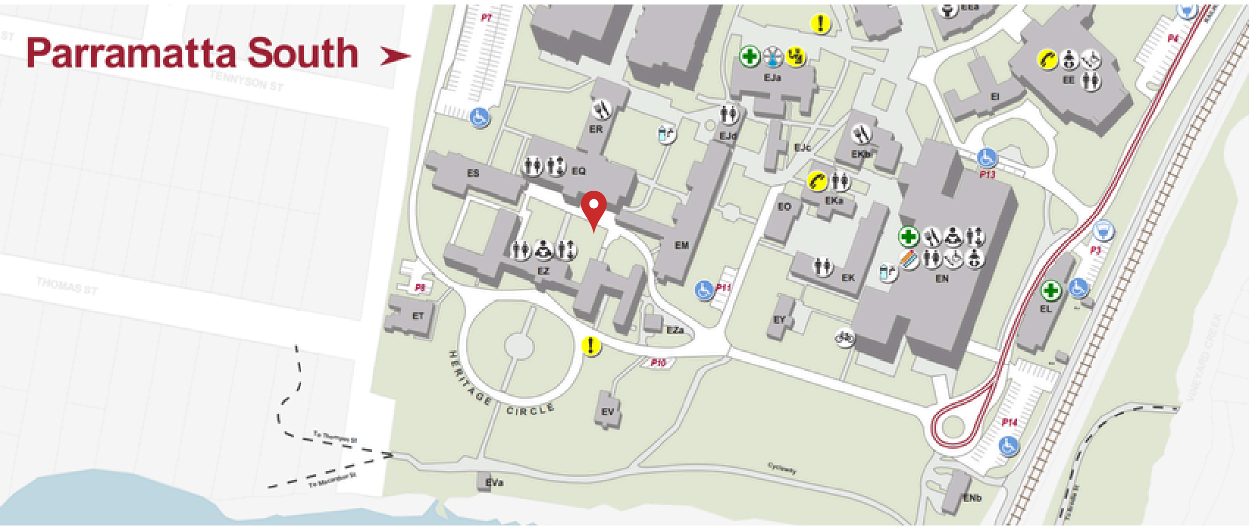
COMPLIANCE REPRESENTATIVES & COMPLIANCE CONTACTS

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 on its Compliance Management Program. This Manual is written for Designated Compliance Representatives, and their Nominated Compliance Contacts.

It is designed to provide these roles with the essential information, walk-through processes, and resources needed to ensure they can clearly understand and work within the Compliance Management Program, and the Enterprise Risk Management system it is hosted on in order to enable and assure of legislative compliance within their operating area.

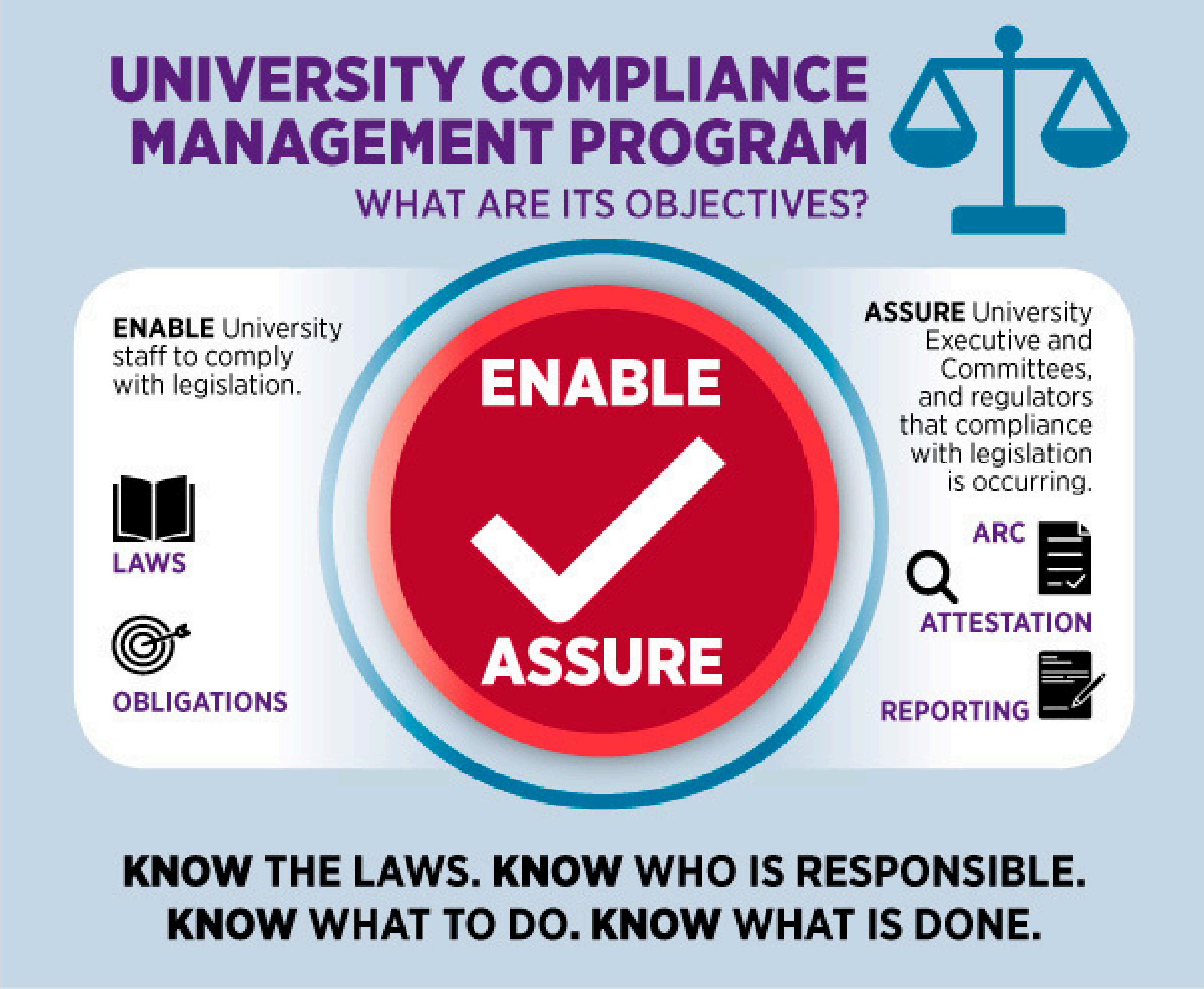
Whether you are a first-time user or experienced with the Program, this Manual is designed to be a practical resource.

I encourage you to read through the sections that are most relevant to your roles and tasks (marked with a ★) and don't hesitate to refer back to this Manual whenever you need assistance. The CPU also welcomes all questions, calls, and emails in our efforts to support you.

Our goal is to make your experience as seamless and efficient as possible, enabling you to achieve the University’s and Controlled Entities’ assurance activities with confidence.

TABLE OF CONTENTS

1. OBJECTIVES



UNIVERSITY COMPLIANCE MANAGEMENT PROGRAM

WHAT ARE ITS OBJECTIVES?

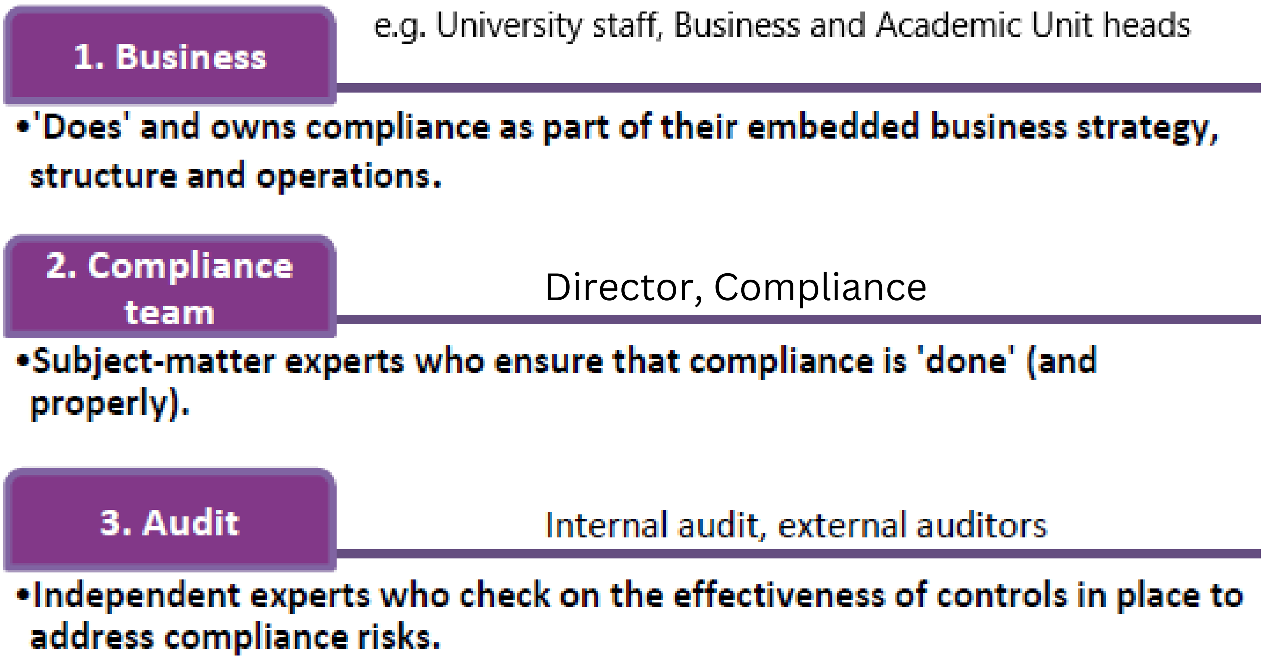
ENABLE University staff to comply with legislation.

ASSURE University Executive and Committees, and regulators that compliance with legislation is occurring.

KNOW THE LAWS. KNOW WHO IS RESPONSIBLE. KNOW WHAT TO DO. KNOW WHAT IS DONE.

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"

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.

SEE RASCI CHART ON PAGE 21

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)

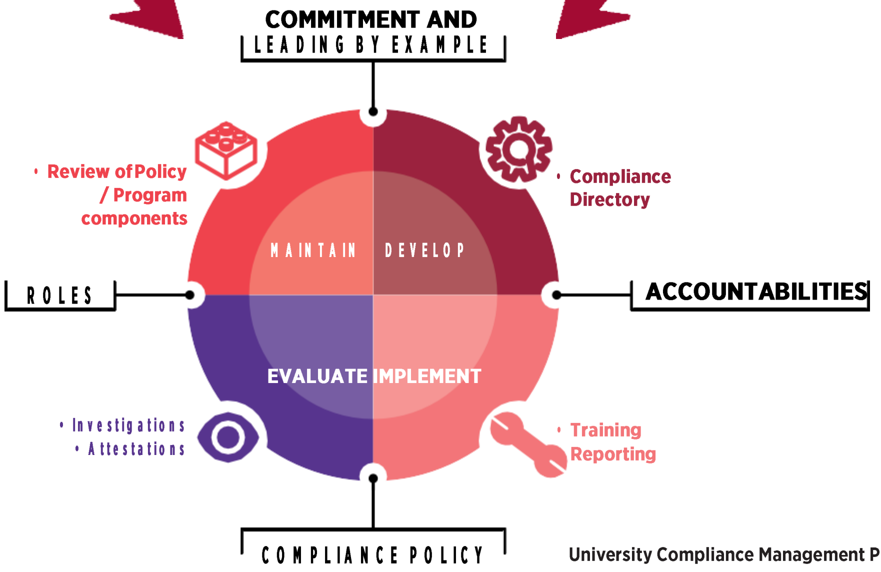
- Assigned Directory laws as it relates to their knowledge of particular operations
- Monitors & annually reviews the Directory for changes to assigned laws & the key obligations
- Reports all actual/potential breaches of & in their area to the CPU
- Promptly investigates & remediates actual/potential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



University Compliance Management Program

ASSURE

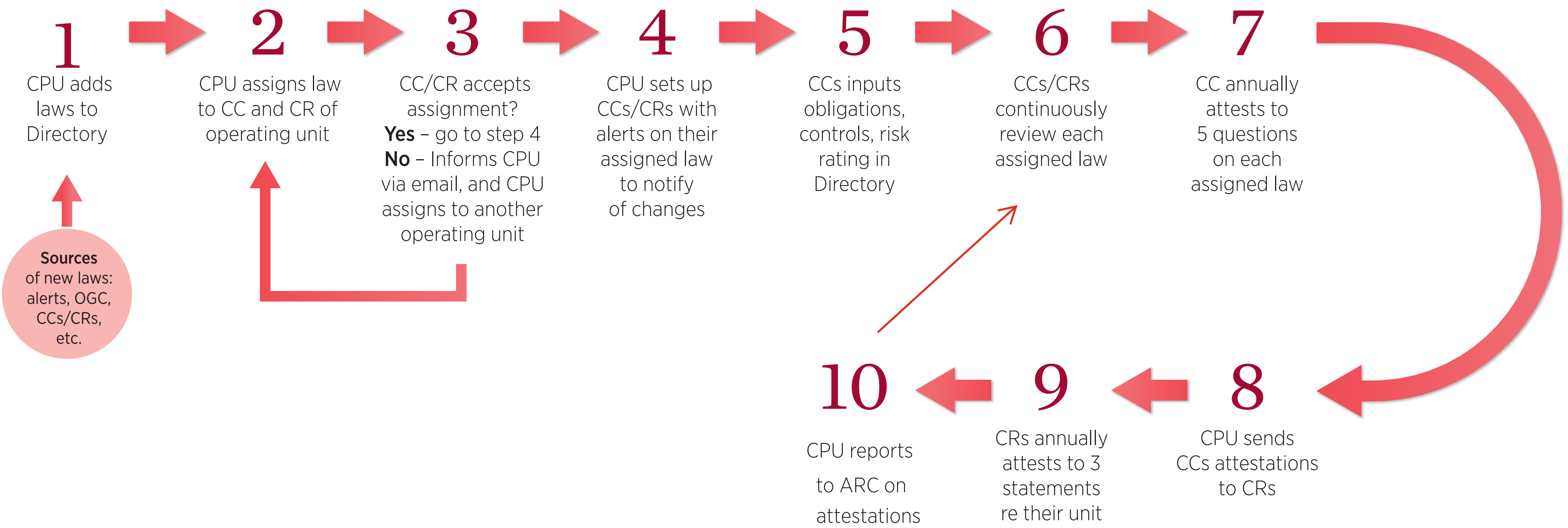
COMPLIANCE SHOULD NOT CHANGE YOUR JOB.

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.

WESTERN SYDNEY
UNIVERSITY

UNIVERSITY COMPLIANCE DIRECTORY AND ANNUAL ATTESTATION PROCESS



1 CPU adds laws to Directory

Sources of new laws: alerts, OGC, CCs/CRs, etc.

2 CPU assigns law to CC and CR of operating unit

3 CC/CR accepts assignment?
Yes – go to step 4
No – Informs CPU via email, and CPU assigns to another operating unit

4 CPU sets up CCs/CRs with alerts on their assigned law to notify of changes

5 CCs inputs obligations, controls, risk rating in Directory

6 CCs/CRs continuously review each assigned law

7 CC annually attests to 5 questions on each assigned law

8 CPU sends CCs attestations to CRs

9 CRs annually attests to 3 statements re their unit

10 CPU reports to ARC on attestations

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

4. KEY DATES

FEBRUARY

- CPU's **formal biannual review** of Compliance Directory and assignments
- Legislative alert refresher training (*upon request*)

MAY

- Compliance Program Unit (CPU) **reports** to Audit and Risk Committee on previous year's attestations.

JULY

- CPU's **formal biannual review** of Compliance Directory and assignments
- Legislative alert refresher training (*upon request*)

SEPTEMBER

- CPU emails **assigned laws confirmation** to Compliance Network - corrections **due** to CPU by end of the month.

OCTOBER

- **Compliance Contact annual attestation** commences on the online University Risk and Compliance system (system).

NOVEMBER

- Compliance Contact attestation **due** for completion by the end of the month on the online system.

NOVEMBER

- **Compliance Representative annual attestation** commences on the online system.

DECEMBER

- **Compliance Representative annual attestation** due for completion by the end of the month on the online system.

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 lists all NSW and Australian Commonwealth laws applicable to the University and/or its Controlled Entities.

Laws may apply due to university structure, operations, activity, revenue, charity status.

Only proactive obligations are captured i.e. the entity must do x, the entity must not do y.

Includes a Watchlist of instruments that set up authority / waiting for assent/commencement, foreign legislation.

WHO DOES THIS?

Compliance Program Unit.

WHAT DO THEY DO?

- Adding applicable legislation to the Directory.
- Noting the relevance to the University and The College.
- Noting the applicability and management of compliance across the enterprise.
- Assessing inherent risk of non-compliance.
- Assigning accountability and watchlist status to operational units.

WHEN DOES THIS OCCUR?

At any time during the calendar year.

How Compliance Contacts/Representatives can support:

Notify the CPU immediately of any law to be added to or removed from the Directory or Watchlist.

5. WORKFLOW DEEP DIVE *STEPS 2 & 3 - ACCOUNTABILITY*

WHAT IS THIS?

Each law on the Compliance Directory is assigned to the unit/s that have ownership of the operational compliance, controls, and procedures as it pertains to the subject matter of the assigned law.

Each law has a designated Compliance Representative aka accountable owner, usually the head of a portfolio.

The Compliance Representative nominates a Compliance Contact aka subject matter expert no lower than a HEW 9, usually a unit head.

WHO DOES THIS?

Compliance Program Unit.

WHAT DO THEY DO?

- Discussing Assignments of accountability with the potential designated area/s and the University General Counsel if applicable prior to formal assignment.
- Assigning accountability of the law in the Directory which will notify via a system generated automated email.
- Escalating to the Senior Executive Team via the University General Counsel for decision if the designated area disagrees with the assignment of accountability.

WHEN DOES THIS OCCUR?

At any time during the calendar year.

How Compliance Contacts/Representatives can support:

Notify the CPU immediately if the assignment of accountability is incorrect, suggesting the correct area.

5. WORKFLOW DEEP DIVE

STEP 4 - EMAIL ALERTS

WHAT IS THIS?

Monitoring any changes (amendments, repeals etc) to laws is essential for operational compliance.

Unmonitored legislative changes expose the University to high risk of non-compliance, resulting in adverse consequences such as penalties, imprisonment, and reputational impact.

Setting up legislative email alerts for the compliance representative and the compliance contact ensures the accountable operating area has at least one resource to monitor any changes (amendments, repeals etc) to the assigned law.

WHO DOES THIS?

Compliance Program Unit.

WHAT DO THEY DO?

- Adding Designated Compliance Representatives and Nominated Compliance Contacts to the legislative alerts service for each of their assigned laws.

WHEN DOES THIS OCCUR?

Immediately after assignment of accountability.

★

How Compliance Contacts/Representatives can support:

Monitor your assigned laws by reading and actioning your legislative email alerts as they come in.

5. WORKFLOW DEEP DIVE
STEP 5 – SELF-ASSESSMENT

WHAT IS THIS?

The self-assessment is the evidence of assessing the non-compliance risk of assigned legislation.

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

★

WHO DOES THIS?

Nominated Compliance Contact

WHAT DO THEY DO?

Self-assessment entails 4 tasks:

1. Listing the compliance obligations
2. Confirming the compliance status of each obligation
3. Entering the controls that mitigate the non-compliance risk of the compliance obligations
4. Assessing the residual risk of non-compliance after controls are executed

WHEN DOES THIS OCCUR?

Within 30 days of assignment of accountability, structural change, or regulatory amendments.

How the Compliance Program Unit can support:

- Review your self-assessment for accuracy in obligations
- Assess the design effectiveness of your mitigating controls
- Provide feedback on the residual risk assessment

5. WORKFLOW DEEP DIVE

STEP 6 –

CONTINUAL REVIEW

WHAT IS THIS?

Continual review assists in a smooth process for Annual Attestation.

Not monitoring and reviewing your assigned laws affects the overall non-compliance risk assessment, and compliance status of your obligations.

The number and risk of non-compliance incidents (especially if not managed and closed) affects the overall non-compliance risk assessment.

WHO DOES THIS?

Nominated Compliance Contact

WHAT DO THEY DO?

- Monitoring assigned laws for any changes as they come in.
- Updating the self-assessment's obligations, compliance status, controls, and residual risk assessment in response.
- Reporting on non-compliance incidents to assigned laws as they occur.
- Managing the non-compliance incident including information on immediate corrective actions, prevention recurrence mitigation, root cause analysis, and uploading evidence.
- Communicating and updating these changes such as training and policies.

WHEN DOES THIS OCCUR?

At any time when there is an amendment or non-compliance incident.

How the Compliance Program Unit can support:

- Assist in reading your legislative alerts.
- Advise on whom to communicate and what documents to update.

5. WORKFLOW DEEP DIVE

STEP 7 –

COMPLIANCE CONTACT ANNUAL ATTESTATION

WHAT IS THIS?
Annual attestation simply verifies the self-assessment and continual review to ensure the currency of the overall non-compliance risk assessment.

Annual attestation also assures the Board of Trustees that there is no material non-compliance of the assigned laws in their operating areas that could adversely affect the University’s ability to comply with legislative requirements.

WHO DOES THIS?
Nominated Compliance Contact

WHAT DO THEY DO?
Answer all attestation questions in the relevant section.

WHEN DOES THIS OCCUR?
October to November, in the date span as notified by the CPU.

How the Compliance Program Unit can support:

- Assist in inputting onto the enterprise risk and compliance system.
- Guide you on your attestation.
- Remind you of completion dates.

5. WORKFLOW DEEP DIVE
STEP 8 –
CPU VALIDATION

WHAT IS THIS?

Independent quality assurance and cross-corroboration of each Compliance Contacts' annual attestation to ensure the accuracy of the overall non-compliance risk assessment.

WHO DOES THIS?

Compliance Program Unit

WHAT DO THEY DO?

The CPU reviews each submitted attested assigned law to ensure the Contact has:

1. Accurately answered each attestation question, such as reporting on non-compliance incidents or confirming compliance status.
2. Appropriately answered the question on residual risk of non-compliance by cross-verifying to the compliance incident breach register to determine, if any, the status and risk severity of the incident.

WHEN DOES THIS OCCUR?

After each Nominated Compliance Contact annual attestation is submitted and prior to the Designated Compliance Representative annual attestation.

★

How Compliance Contacts/Representatives can support:

- Answer any questions from the CPU.
- Confirm any changes to be made to your attestations.

5. WORKFLOW DEEP DIVE STEP 9 – *COMPLIANCE REPRESENTATIVE ANNUAL ATTESTATION*

WHAT IS THIS?

Compliance Representative attestation assures of no material non-compliance risk across the wider portfolio and embodies the segregation of duties control.

WHO DOES THIS?

Designated Compliance Representative

WHAT DO THEY DO?

Answer all attestation questions in the relevant section.

WHEN DOES THIS OCCUR?

November to December, after the CPU notifies with a summary of every submitted annual attestation in their portfolio.

How the Compliance Program Unit can support:

- Assist in inputting onto the enterprise risk and compliance system.
- Guide you on your attestation.
- Remind you of completion dates.

5. WORKFLOW DEEP DIVE
STEP 10 –
ARC REPORTING

WHAT IS THIS?

Independent papers are submitted to the sub-committee of the Board of Trustees, the Audit and Risk Committee, outlining the results from the enabling and assurance activities of the compliance framework.

WHO DOES THIS?

Compliance Program Unit

WHAT DO THEY DO?

The CPU outlines:

1. any assigned law above the university's risk appetite for legislative non-compliance risk, which is "Low".
2. any portfolio with outstanding attestations, which reverts their assigned laws to the inherent risk rating (which is always above the risk appetite).
3. any HIGH-RISK compliance issues identified from the attestation process.

WHEN DOES THIS OCCUR?

When the annual report is scheduled, usually in Quarter 1 of the next calendar year.

How Compliance Contacts/Representatives can support:

Complete all attestations by the due date to not be mentioned in the report as an outstanding infraction.

5. WORKFLOW DEEP DIVE *INTERACTIVE LINKS*

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

5. WORKFLOW DEEP DIVE

IMPORTANT LINKS

COMPLIANCE PROGRAM UNIT WEBSITE

COMPLIANCE POLICY

COMPLIANCE DIRECTORY

FACTSHEETS

- See RASCI chart overleaf

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	COMPLIANCE PROGRAM UNIT	COMPLIANCE REPRESENTATIVE	COMPLIANCE CONTACT	ALL STAFF
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	COMPLIANCE PROGRAM UNIT	COMPLIANCE REPRESENTATIVE	COMPLIANCE CONTACT	ALL STAFF
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

6. PROCESS DOCUMENTS

STEP 4

LAWONE LEGISLATIVE EMAIL ALERTS

PAGE 26-30

INSTRUCTIONS ON HOW TO ACCESS ALERTS AND GENERATE REPORTS

STEP 5

SELF-ASSESSMENT

PAGE 31-43

INSTRUCTIONS ON WHEN AND HOW TO COMPLETE INCLUDING HOW TO WRITE CONTROL STATEMENTS (PAGE 39)

STEP 6

COMPLIANCE INCIDENT REPORTING

PAGE 44-51

INSTRUCTIONS ON HOW TO COMPLETE INCLUDING HOW TO CONDUCT A ROOT CAUSE ANALYSIS (PAGE 49)

STEPS 7 & 9

ANNUAL ATTESTATION

PAGE 52-64

INSTRUCTIONS ON HOW TO COMPLETE FOR
A COMPLIANCE CONTACT (PAGE 52)
A COMPLIANCE REPRESENTATIVE (PAGE 64)

WESTERN SYDNEY
UNIVERSITY

Compliance Management Program – 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

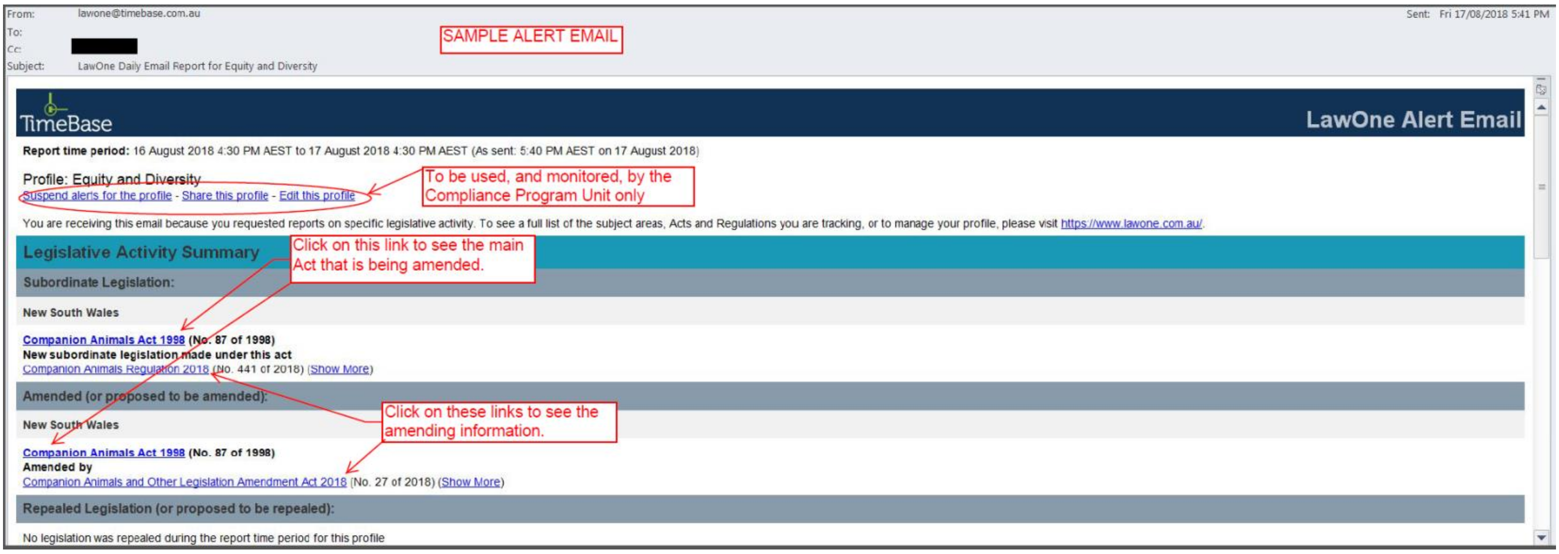
3. There is one alert per assigned law on the Compliance Directory, sent on the day of the amendment.

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.



From: lawone@timebase.com.au
Sent: Fri 17/08/2018 5:41 PM
To: [redacted]
Cc:
Subject: LawOne Daily Email Report for Equity and Diversity

SAMPLE ALERT EMAIL

TimeBase
LawOne Alert Email

Report time period: 16 August 2018 4:30 PM AEST to 17 August 2018 4:30 PM AEST (As sent: 5:40 PM AEST on 17 August 2018)

Profile: Equity and Diversity
Suspend alerts for the profile - Share this profile - Edit this profile

To be used, and monitored, by the Compliance Program Unit only

You are receiving this email because you requested reports on specific legislative activity. To see a full list of the subject areas, Acts and Regulations you are tracking, or to manage your profile, please visit https://www.lawone.com.au/.

Legislative Activity Summary

Click on this link to see the main Act that is being amended.

Subordinate Legislation:

New South Wales

Companion Animals Act 1998 (No. 87 of 1998)
New subordinate legislation made under this act
Companion Animals Regulation 2018 (No. 441 of 2018) (Show More)

Amended (or proposed to be amended):

Click on these links to see the amending information.

New South Wales

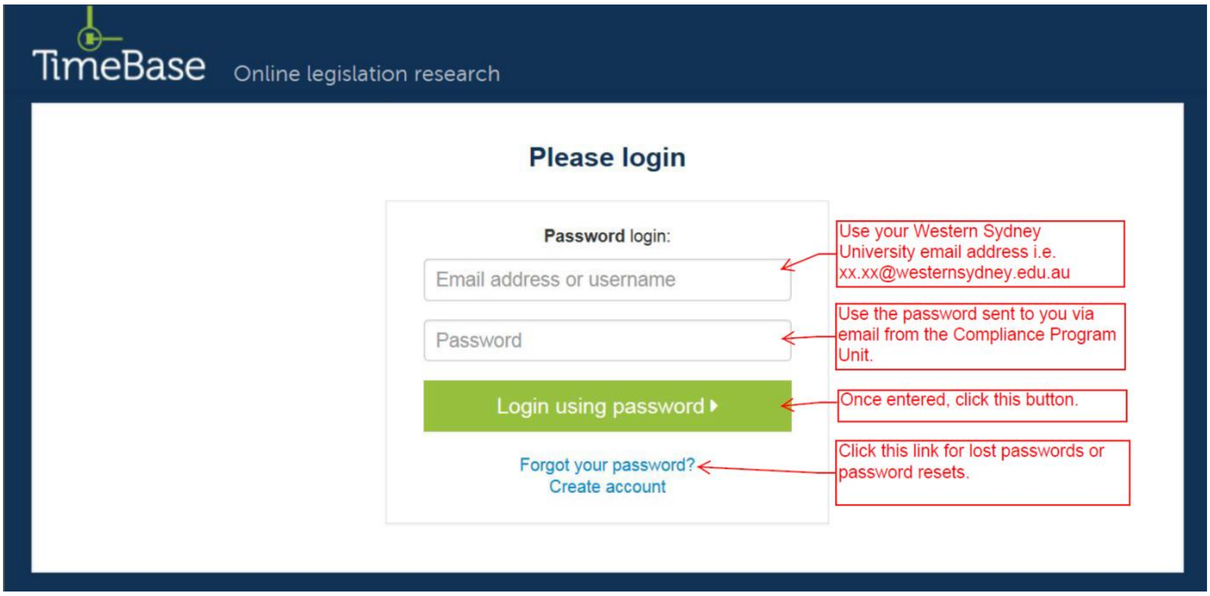
Companion Animals Act 1998 (No. 87 of 1998)
Amended by
Companion Animals and Other Legislation Amendment Act 2018 (No. 27 of 2018) (Show More)

Repealed Legislation (or proposed to be repealed):

No legislation was repealed during the report time period for this profile

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.



Use your Western Sydney University email address i.e. xx.xx@westernsydney.edu.au

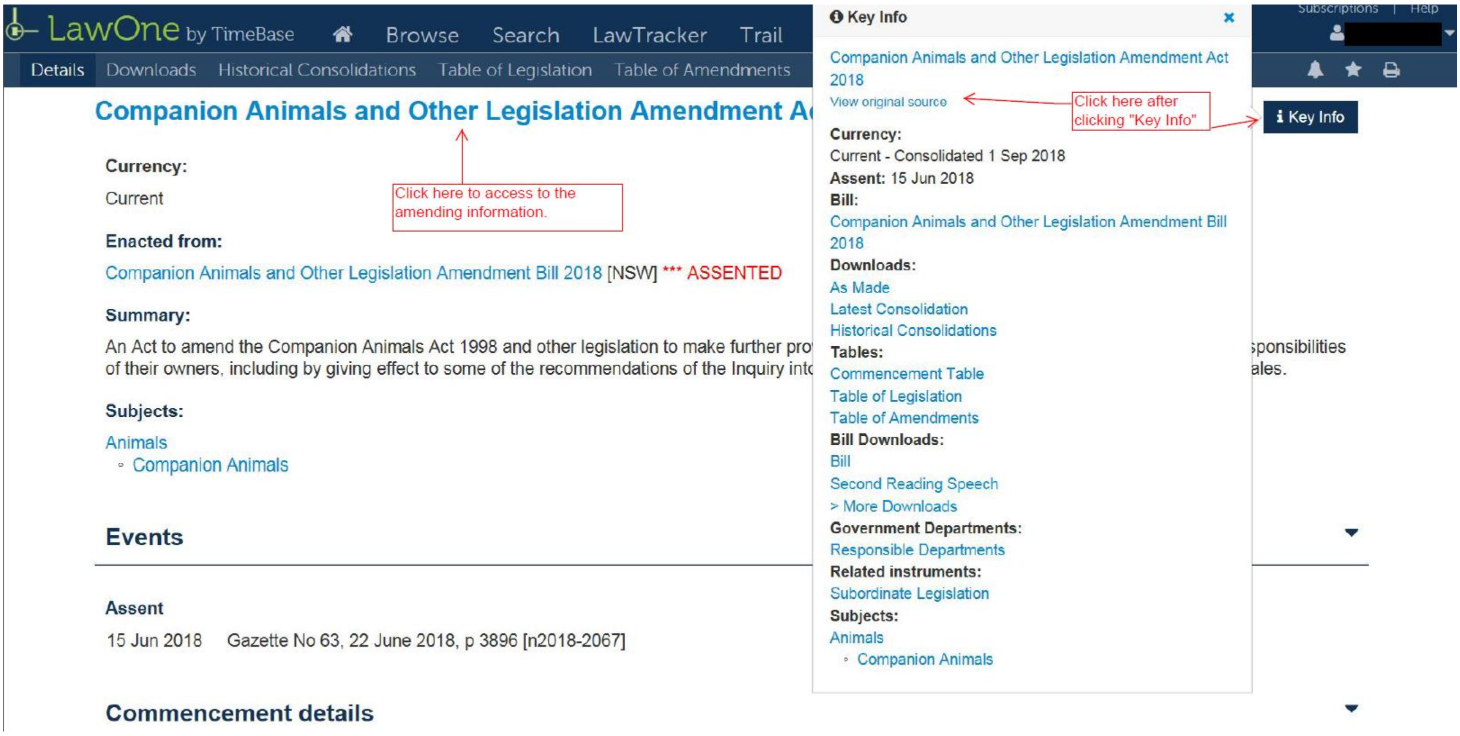
Use the password sent to you via email from the Compliance Program Unit.

Once entered, click this button.

Click this link for lost passwords or password resets.

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”.



Companion Animals and Other Legislation Amendment A

Click here to access to the amending information.

Currency:
Current

Enacted from:
Companion Animals and Other Legislation Amendment Bill 2018 [NSW] *** ASSENTED

Summary:
An Act to amend the Companion Animals Act 1998 and other legislation to make further pro ... sponsibilities of their owners, including by giving effect to some of the recommendations of the Inquiry into ... ales.

Subjects:
Animals
◦ Companion Animals

Events

Assent
15 Jun 2018 Gazette No 63, 22 June 2018, p 3896 [n2018-2067]

Commencement details

ℹ **Key Info** ×

Companion Animals and Other Legislation Amendment Act 2018
View original source

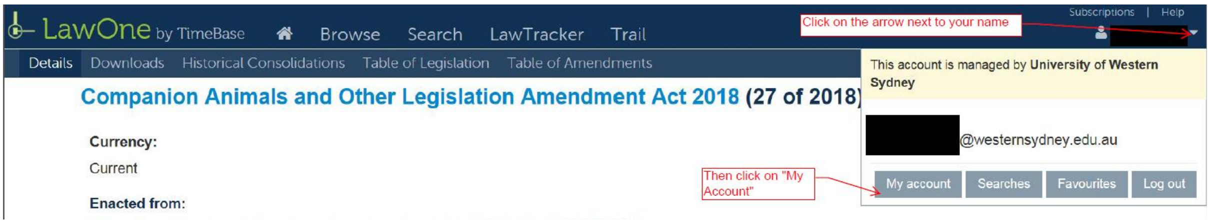
Click here after clicking "Key Info"

Currency:
Current - Consolidated 1 Sep 2018
Assent: 15 Jun 2018
Bill:
Companion Animals and Other Legislation Amendment Bill 2018
Downloads:
As Made
Latest Consolidation
Historical Consolidations
Tables:
Commencement Table
Table of Legislation
Table of Amendments
Bill Downloads:
Bill
Second Reading Speech
> More Downloads
Government Departments:
Responsible Departments
Related instruments:
Subordinate Legislation
Subjects:
Animals
◦ Companion Animals

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.



Click on the arrow next to your name

[redacted]

Companion Animals and Other Legislation Amendment Act 2018 (27 of 2018)

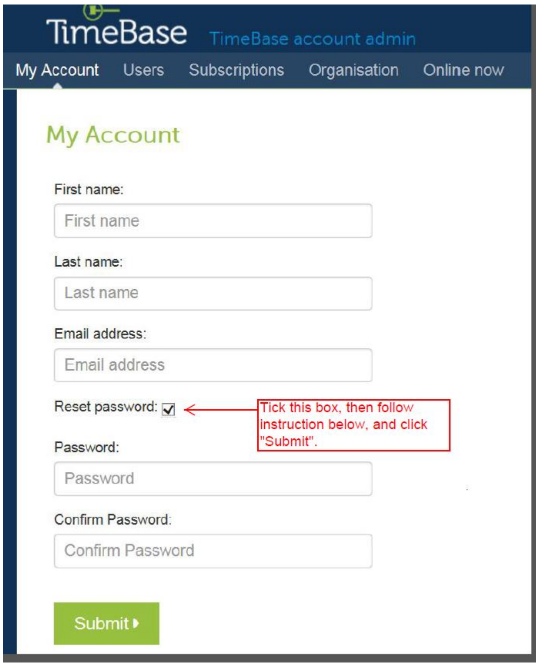
Currency:
Current

Enacted from:

This account is managed by **University of Western Sydney**

[redacted]@westernsydney.edu.au

Then click on "My Account"



My Account

First name: First name

Last name: Last name

Email address: Email address

Reset password: ☑

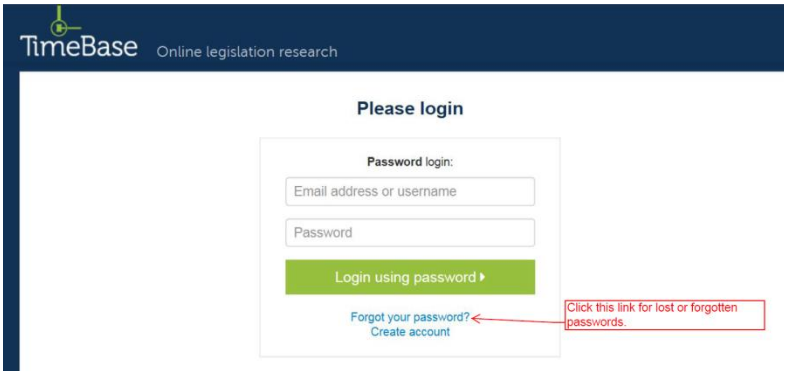
Tick this box, then follow instruction below, and click "Submit".

Password: Password

Confirm Password: Confirm Password

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.



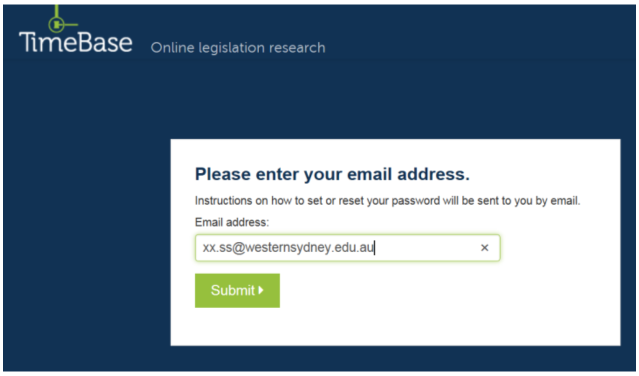
Please login

Password login:

Email address or username

Password

Click this link for lost or forgotten passwords.

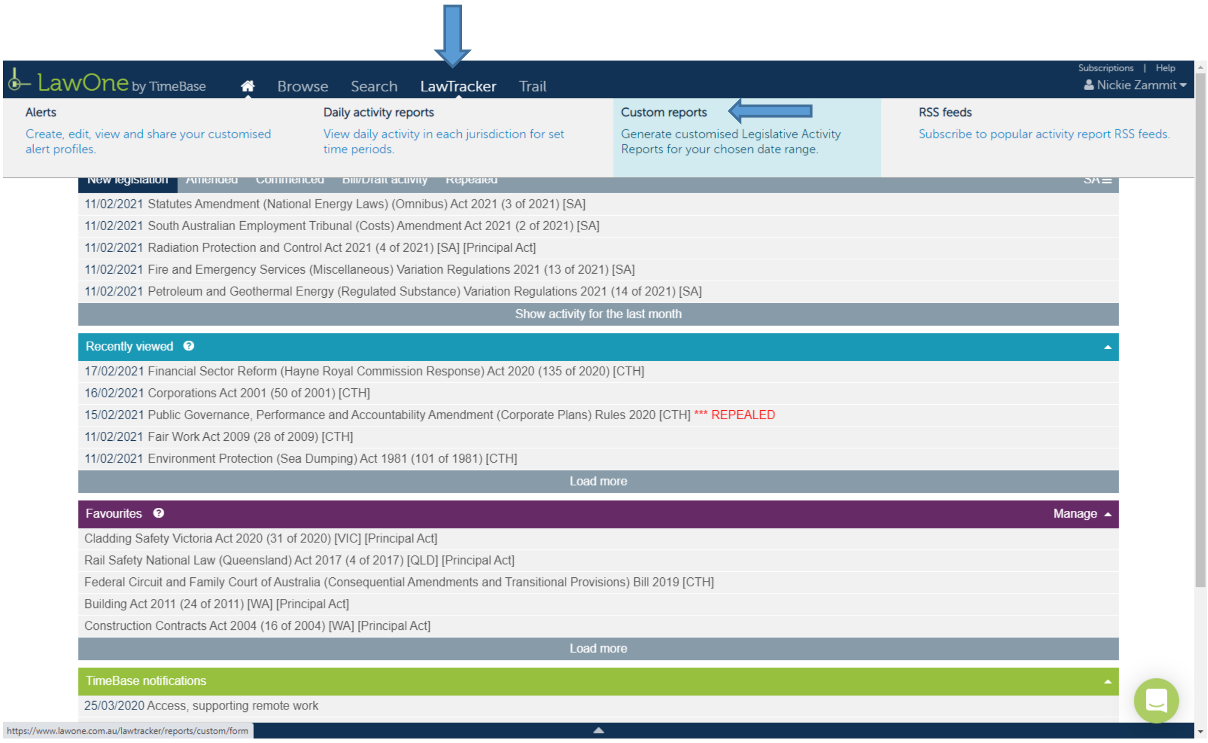


Please enter your email address.

Instructions on how to set or reset your password will be sent to you by email.

Email address: xx.ss@westernsydney.edu.au ×

To run custom reports on an Existing Profile make sure you are Login as yourself click on the LAWTRACKER tab then choose CUSTOM REPORTS.



Alerts

Create, edit, view and share your customised alert profiles.

Daily activity reports

View daily activity in each jurisdiction for set time periods.

Custom reports

Generate customised Legislative Activity Reports for your chosen date range.

RSS feeds

Subscribe to popular activity report RSS feeds.

11/02/2021 Statutes Amendment (National Energy Laws) (Omnibus) Act 2021 (3 of 2021) [SA]
11/02/2021 South Australian Employment Tribunal (Costs) Amendment Act 2021 (2 of 2021) [SA]
11/02/2021 Radiation Protection and Control Act 2021 (4 of 2021) [SA] [Principal Act]
11/02/2021 Fire and Emergency Services (Miscellaneous) Variation Regulations 2021 (13 of 2021) [SA]
11/02/2021 Petroleum and Geothermal Energy (Regulated Substance) Variation Regulations 2021 (14 of 2021) [SA]

Recently viewed

17/02/2021 Financial Sector Reform (Hayne Royal Commission Response) Act 2020 (135 of 2020) [CTH]
16/02/2021 Corporations Act 2001 (50 of 2001) [CTH]
15/02/2021 Public Governance, Performance and Accountability Amendment (Corporate Plans) Rules 2020 [CTH] *** REPEALED
11/02/2021 Fair Work Act 2009 (28 of 2009) [CTH]
11/02/2021 Environment Protection (Sea Dumping) Act 1981 (101 of 1981) [CTH]

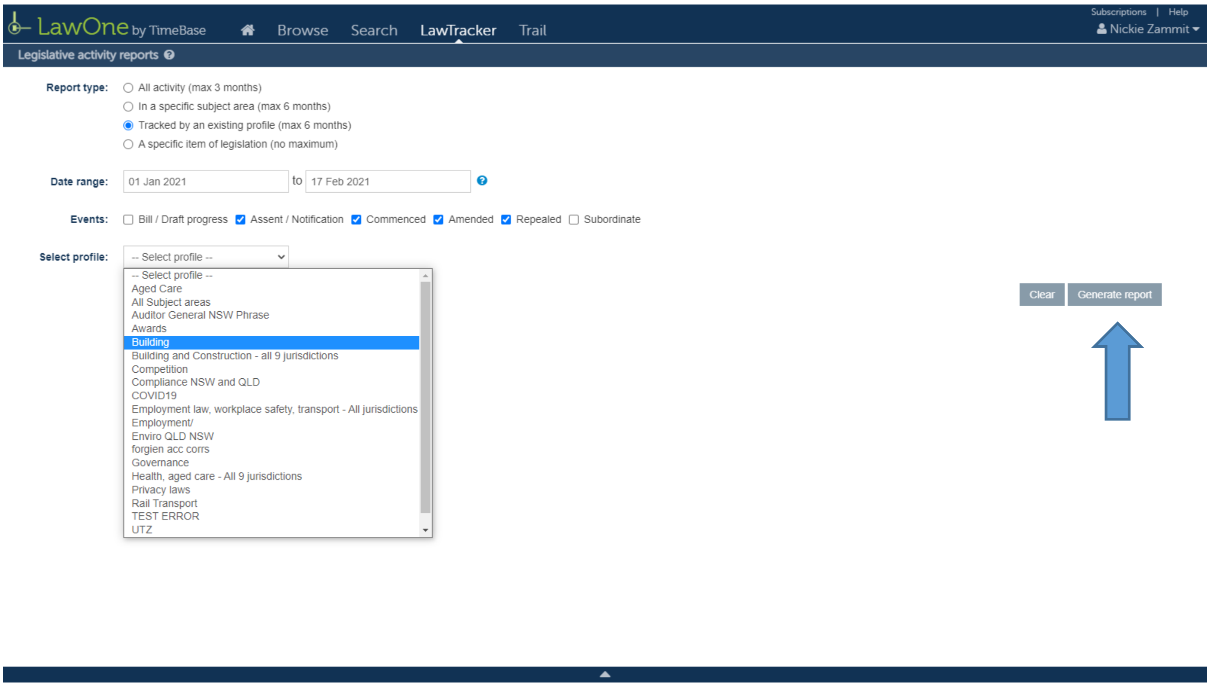
Favourites

Cladding Safety Victoria Act 2020 (31 of 2020) [VIC] [Principal Act]
Rail Safety National Law (Queensland) Act 2017 (4 of 2017) [QLD] [Principal Act]
Federal Circuit and Family Court of Australia (Consequential Amendments and Transitional Provisions) Bill 2019 [CTH]
Building Act 2011 (24 of 2011) [WA] [Principal Act]
Construction Contracts Act 2004 (16 of 2004) [WA] [Principal Act]

TimeBase notifications

25/03/2020 Access, supporting remote work

Tick the TRACKED BY AN EXISTING PROFILE Enter in the date range make sure you choose all the events you which to report on then select your profile from the drop down box then Click GENERATE REPORT.



Legislative activity reports

Report type:
○ All activity (max 3 months)
○ In a specific subject area (max 6 months)
● Tracked by an existing profile (max 6 months)
○ A specific item of legislation (no maximum)

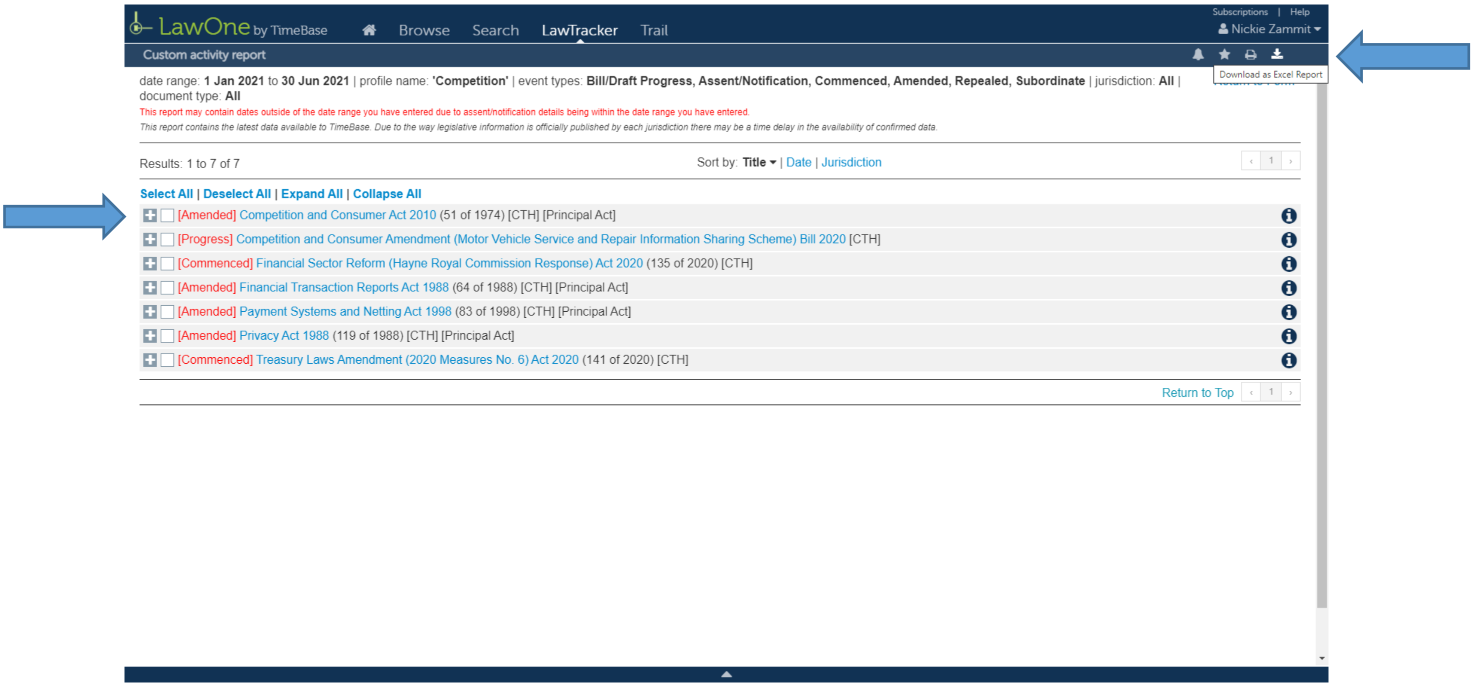
Date range: 01 Jan 2021 to 17 Feb 2021

Events: □ Bill / Draft progress ☑ Assent / Notification ☑ Commenced ☑ Amended ☑ Repealed □ Subordinate

Select profile: -- Select profile --

-- Select profile --
Aged Care
All Subject areas
Auditor General NSW Phrase
Awards
Building
Building and Construction - all 9 jurisdictions
Competition
Compliance NSW and QLD
COVID19
Employment law, workplace safety, transport - All jurisdictions
Employment/
Enviro QLD NSW
forgien acc corrs
Governance
Health, aged care - All 9 jurisdictions
Privacy laws
Rail Transport
TEST ERROR
UTZ

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.



date range: **1 Jan 2021** to **30 Jun 2021** | profile name: **'Competition'** | event types: **Bill/Draft Progress, Assent/Notification, Commenced, Amended, Repealed, Subordinate** | jurisdiction: **All** | document type: **All**

This report may contain dates outside of the date range you have entered due to assent/notification details being within the date range you have entered.

This report contains the latest data available to TimeBase. Due to the way legislative information is officially published by each jurisdiction there may be a time delay in the availability of confirmed data.

Results: 1 to 7 of 7

Sort by: **Title** | Date | Jurisdiction

Select All | **Deselect All** | **Expand All** | **Collapse All**

- ⊞ □ [Amended] Competition and Consumer Act 2010 (51 of 1974) [CTH] [Principal Act]
- ⊞ □ [Progress] Competition and Consumer Amendment (Motor Vehicle Service and Repair Information Sharing Scheme) Bill 2020 [CTH]
- ⊞ □ [Commenced] Financial Sector Reform (Hayne Royal Commission Response) Act 2020 (135 of 2020) [CTH]
- ⊞ □ [Amended] Financial Transaction Reports Act 1988 (64 of 1988) [CTH] [Principal Act]
- ⊞ □ [Amended] Payment Systems and Netting Act 1998 (83 of 1998) [CTH] [Principal Act]
- ⊞ □ [Amended] Privacy Act 1988 (119 of 1988) [CTH] [Principal Act]
- ⊞ □ [Commenced] Treasury Laws Amendment (2020 Measures No. 6) Act 2020 (141 of 2020) [CTH]

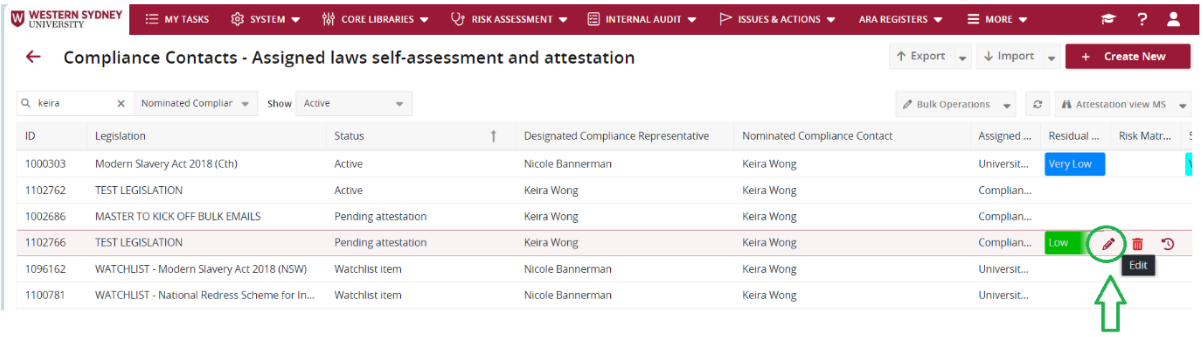
Return to Top

Compliance Management Program Control Self-Assessment Process Document

COMPLETE SELF-ASSESSMENT WITHIN 30 DAYS OF
I) INITIAL ASSIGNMENT;
II) STRUCTURAL CHANGES; AND
III) REGULATORY AMENDMENTS.

A. Access your Dashboard.

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



Compliance Contacts - Assigned laws self-assessment and attestation

keira | Nominated Compliar | Show Active

ID	Legislation	Status	Designated Compliance Representative	Nominated Compliance Contact	Assigned ...	Residual ...	Risk Matr...
1000303	Modern Slavery Act 2018 (Cth)	Active	Nicole Bannerman	Keira Wong	Universit...	Very Low	
1102762	TEST LEGISLATION	Active	Keira Wong	Keira Wong	Complian...		
1002686	MASTER TO KICK OFF BULK EMAILS	Pending attestation	Keira Wong	Keira Wong	Complian...		
1102766	TEST LEGISLATION	Pending attestation	Keira Wong	Keira Wong	Complian...	Low	
1096162	WATCHLIST - Modern Slavery Act 2018 (NSW)	Watchlist item	Nicole Bannerman	Keira Wong	Universit...		
1100781	WATCHLIST - National Redress Scheme for In...	Watchlist item	Nicole Bannerman	Keira Wong	Universit...		

Click the pencil icon to edit the assigned item to complete the attestation

C. Question 2A.

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

i) the obligation (if needed)

ii) compliance status from “Unknown”

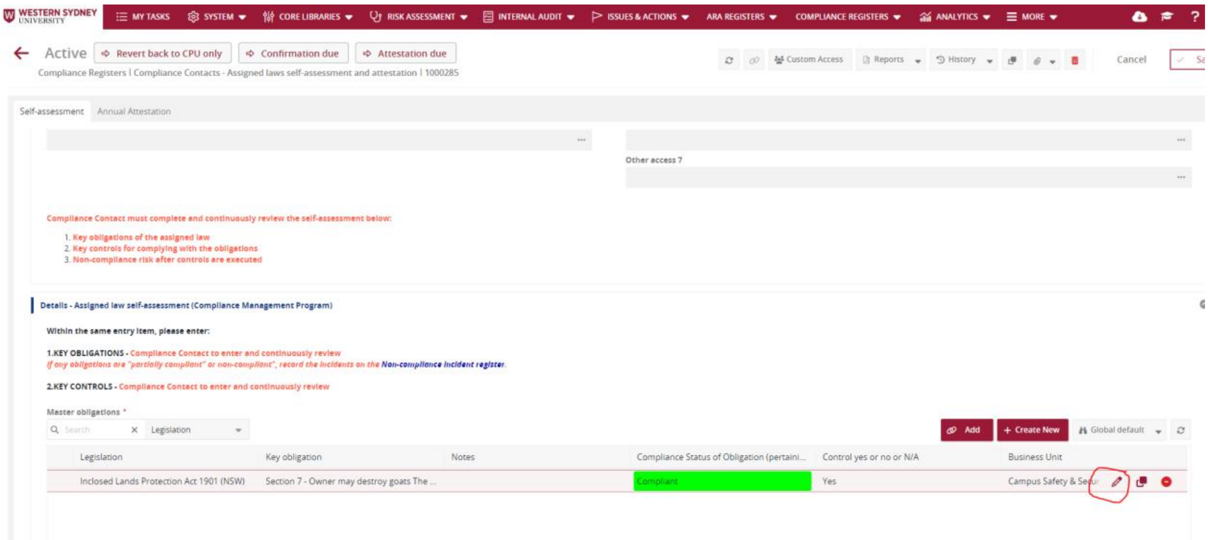
iii) statement of evidence of compliance

iv) attachment of evidence if able

v) controls that mitigate the non-compliance risk, adding more or deleting, as long as it is current and accurate (do not enter controls that aren’t yet executed)

vi) statement of evidence of controls

vii) attachment of evidence if able



Compliance Registers | Compliance Contacts - Assigned laws self-assessment and attestation | 1000285

Other access 7

Compliance Contact must complete and continuously review the self-assessment below:

1. Key obligations of the assigned law
2. Key controls for complying with the obligations
3. Non-compliance risk after controls are executed

Details - Assigned law self-assessment (Compliance Management Program)

Within the same entry item, please enter:

1.KEY OBLIGATIONS - Compliance Contact to enter and continuously review
If any obligations are "partially compliant" or non-compliant", record the incidents on the Non-compliance Incident register.

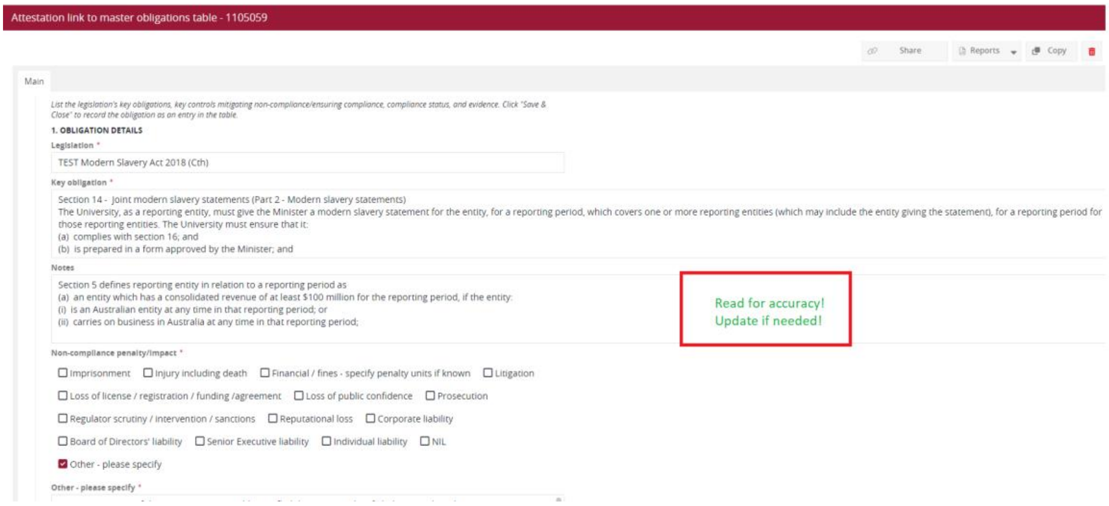
2.KEY CONTROLS - Compliance Contact to enter and continuously review

Master obligations *

Search | Legislation

Legislation	Key obligation	Notes	Compliance Status of Obligation (pertaini...	Control yes or no or N/A	Business Unit
Inclosed Lands Protection Act 1901 (NSW)	Section 7 - Owner may destroy goats The ...		Compliant	Yes	Campus Safety & Secu

i) Read and update the obligation (if needed).



Attestation link to master obligations table - 1105059

List the legislation's key obligations, key controls mitigating non-compliance/ensuring compliance, compliance status, and evidence. Click "Save & Close" to record the obligation as an entry in the table.

1. OBLIGATION DETAILS

Legislation *

TEST Modern Slavery Act 2018 (Cth)

Key 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

Notes

Section 5 defines reporting entity in relation to a reporting period as
(a) an entity which has a consolidated revenue of at least $100 million for the reporting period, if the entity:
(i) is an Australian entity at any time in that reporting period; or
(ii) carries on business in Australia at any time in that reporting period;

Read for accuracy!
Update if needed!

Non-compliance penalty/impact *

☐ Imprisonment ☐ Injury including death ☐ Financial / fines - specify penalty units if known ☐ Litigation

☐ Loss of license / registration / funding /agreement ☐ Loss of public confidence ☐ Prosecution

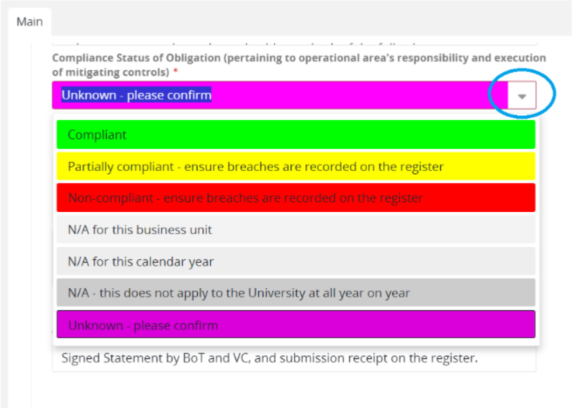
☐ Regulator scrutiny / intervention / sanctions ☐ Reputational loss ☐ Corporate liability

☐ Board of Directors' liability ☐ Senior Executive liability ☐ Individual liability ☐ NIL

☑ Other - please specify

Other - please specify *

ii) Update the compliance status from “Unknown”



Compliance Status of Obligation (pertaining to operational area's responsibility and execution of mitigating controls) *

Unknown - please confirm

- Compliant
- Partially compliant - ensure breaches are recorded on the register
- Non-compliant - ensure breaches are recorded on the register
- N/A for this business unit
- N/A for this calendar year
- N/A - this does not apply to the University at all year on year
- Unknown - please confirm

Signed Statement by BoT and VC, and submission receipt on the register.

Choose the appropriate and correct status option for the calendar year for the obligation, other than "Unknown".

Ensure it reflects your answer in Question 2 above.

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”.

Note: Fields iii) and iv) are not required if the status is marked "N/A…"

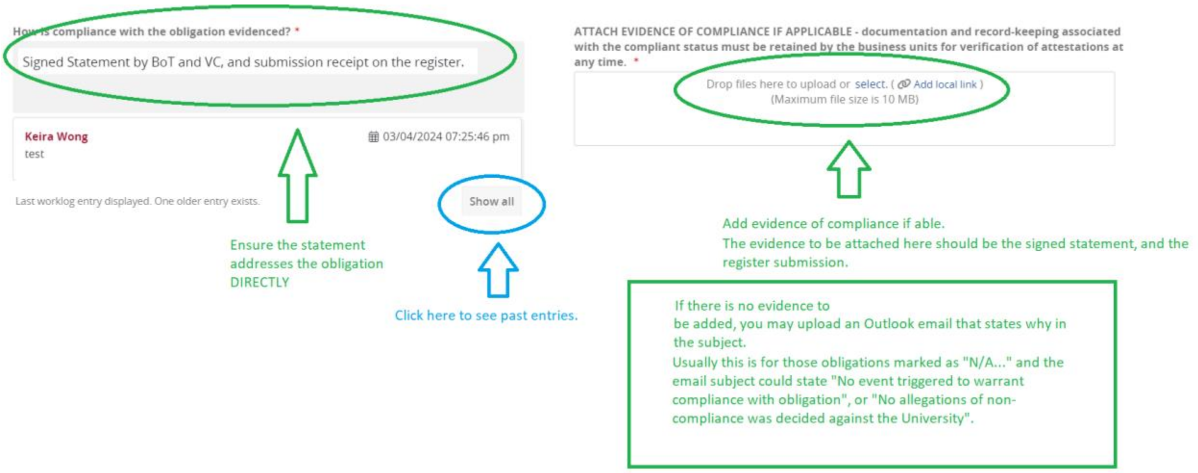
iii) Update the statement of evidence of compliance

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".

iv) Update the attachment of evidence if able

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.



How is compliance with the obligation evidenced? *

Signed Statement by BoT and VC, and submission receipt on the register.

Keira Wong
test

03/04/2024 07:25:46 pm

Last worklog entry displayed. One older entry exists.

Ensure the statement addresses the obligation DIRECTLY

Click here to see past entries.

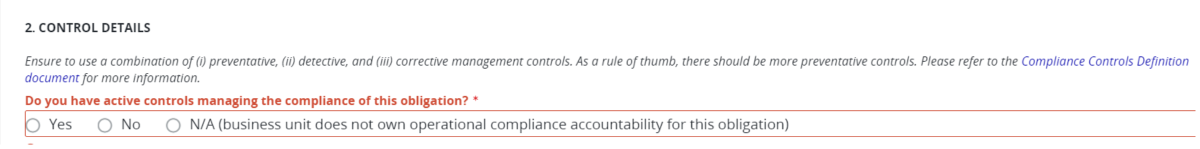
ATTACH EVIDENCE OF COMPLIANCE IF APPLICABLE - documentation and record-keeping associated with the compliant status must be retained by the business units for verification of attestations at any time. *

Drop files here to upload or select. (Add local link)
(Maximum file size is 10 MB)

Add evidence of compliance if able.
The evidence to be attached here should be the signed statement, and the register submission.

If there is no evidence to be added, you may upload an Outlook email that states why in the subject.
Usually this is for those obligations marked as "N/A..." and the email subject could state "No event triggered to warrant compliance with obligation", or "No allegations of non-compliance was decided against the University".

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



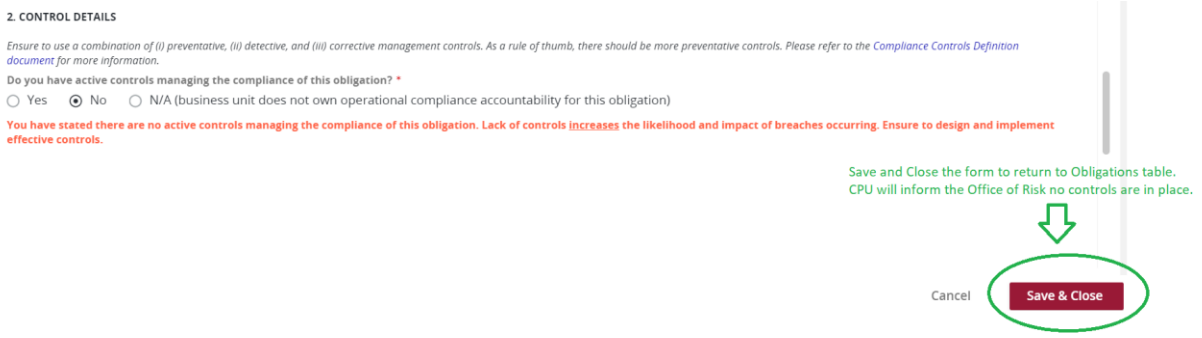
2. CONTROL DETAILS

Ensure to use a combination of (i) preventative, (ii) detective, and (iii) corrective management controls. As a rule of thumb, there should be more preventative controls. Please refer to the Compliance Controls Definition document for more information.

Do you have active controls managing the compliance of this obligation? *

○ Yes ○ No ○ N/A (business unit does not own operational compliance accountability for this obligation)

- 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.



2. CONTROL DETAILS

Ensure to use a combination of (i) preventative, (ii) detective, and (iii) corrective management controls. As a rule of thumb, there should be more preventative controls. Please refer to the Compliance Controls Definition document for more information.

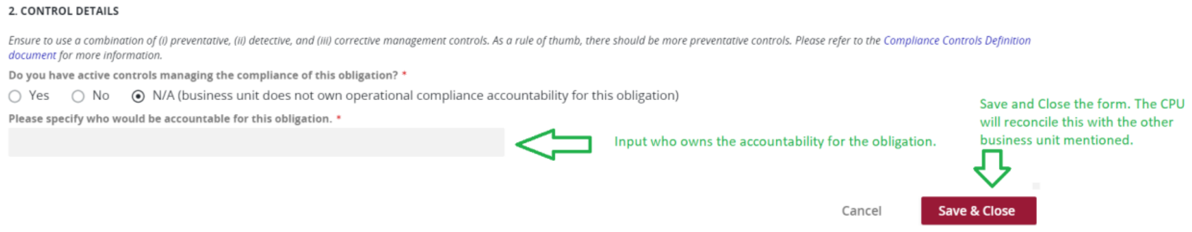
Do you have active controls managing the compliance of this obligation? *

○ Yes ● No ○ N/A (business unit does not own operational compliance accountability for this obligation)

You have stated there are no active controls managing the compliance of this obligation. Lack of controls increases the likelihood and impact of breaches occurring. Ensure to design and implement effective controls.

Save and Close the form to return to Obligations table.
CPU will inform the Office of Risk no controls are in place.

- 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.



2. CONTROL DETAILS

Ensure to use a combination of (i) preventative, (ii) detective, and (iii) corrective management controls. As a rule of thumb, there should be more preventative controls. Please refer to the Compliance Controls Definition document for more information.

Do you have active controls managing the compliance of this obligation? *

○ Yes ○ No ● N/A (business unit does not own operational compliance accountability for this obligation)

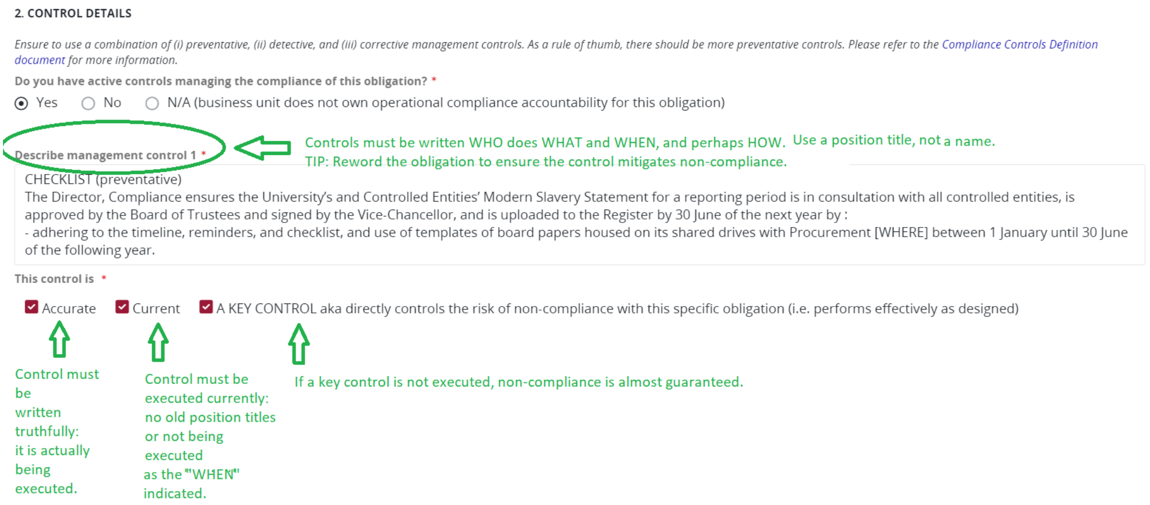
Please specify who would be accountable for this obligation. *

Input who owns the accountability for the obligation.

Save and Close the form. The CPU will reconcile this with the other business unit mentioned.

- 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.
  - There is a Controls Definitions Document linked to help you.

PDF download of Help with Controls



2. CONTROL DETAILS

Ensure to use a combination of (i) preventative, (ii) detective, and (iii) corrective management controls. As a rule of thumb, there should be more preventative controls. Please refer to the Compliance Controls Definition document for more information.

Do you have active controls managing the compliance of this obligation? *

● Yes ○ No ○ N/A (business unit does not own operational compliance accountability for this obligation)

Describe management control 1 *

Controls must be written WHO does WHAT and WHEN, and perhaps HOW. Use a position title, not a name.
TIP: Reword the obligation to ensure the control mitigates non-compliance.

CHECKLIST (preventative)
The Director, Compliance 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 by :
- adhering to the timeline, reminders, and checklist, and use of templates of board papers housed on its shared drives with Procurement [WHERE] between 1 January until 30 June of the following year.

This control is *

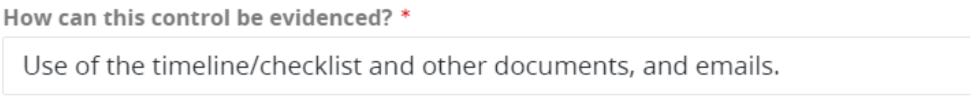
☑ Accurate ☑ Current ☑ A KEY CONTROL aka directly controls the risk of non-compliance with this specific obligation (i.e. performs effectively as designed)

Control must be written truthfully: it is actually being executed.

Control must be executed currently: no old position titles or not being executed as the "WHEN" indicated.

If a key control is not executed, non-compliance is almost guaranteed.

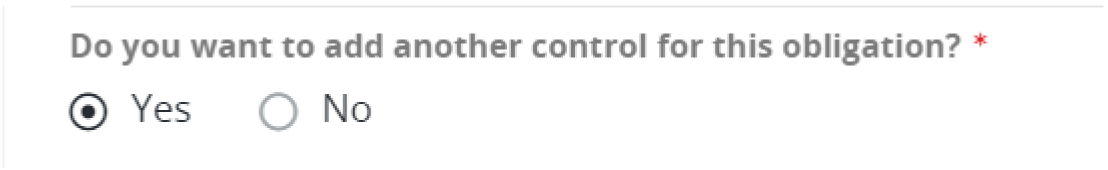
vi) Update the statement of evidence of controls



How can this control be evidenced? *

Use of the timeline/checklist and other documents, and emails.

Ensure the evidence is of the CONTROL, not the compliance. If the control described are reminders, then the evidence of controls are the Outlook calendar reminders or screenshots of.
If it is a checklist, the checklist is listed.



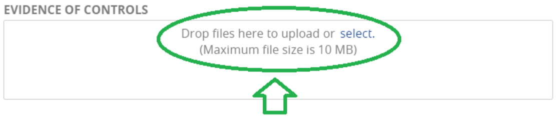
Do you want to add another control for this obligation? *

● Yes ○ No

- 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.

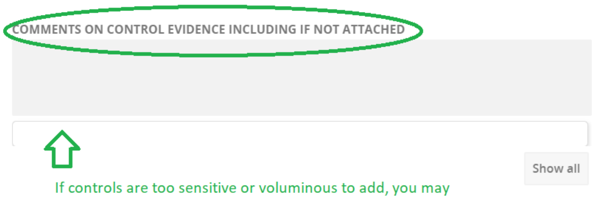
vii) Update the attachment of evidence of controls if able, or comment



EVIDENCE OF CONTROLS

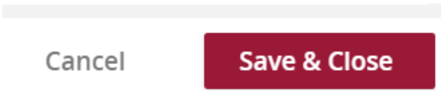
Drop files here to upload or select.
(Maximum file size is 10 MB)

Add evidence of controls. If you listed checklists, you can add the checklists or screenshots of reminders etc



COMMENTS ON CONTROL EVIDENCE INCLUDING IF NOT ATTACHED

If controls are too sensitive or voluminous to add, you may want to add comment as to why they can't be attached, or where they can be located.



- 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

COMPLIANCE INTERNAL CONTROLS
FACTSHEET

(Step 5 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.

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.

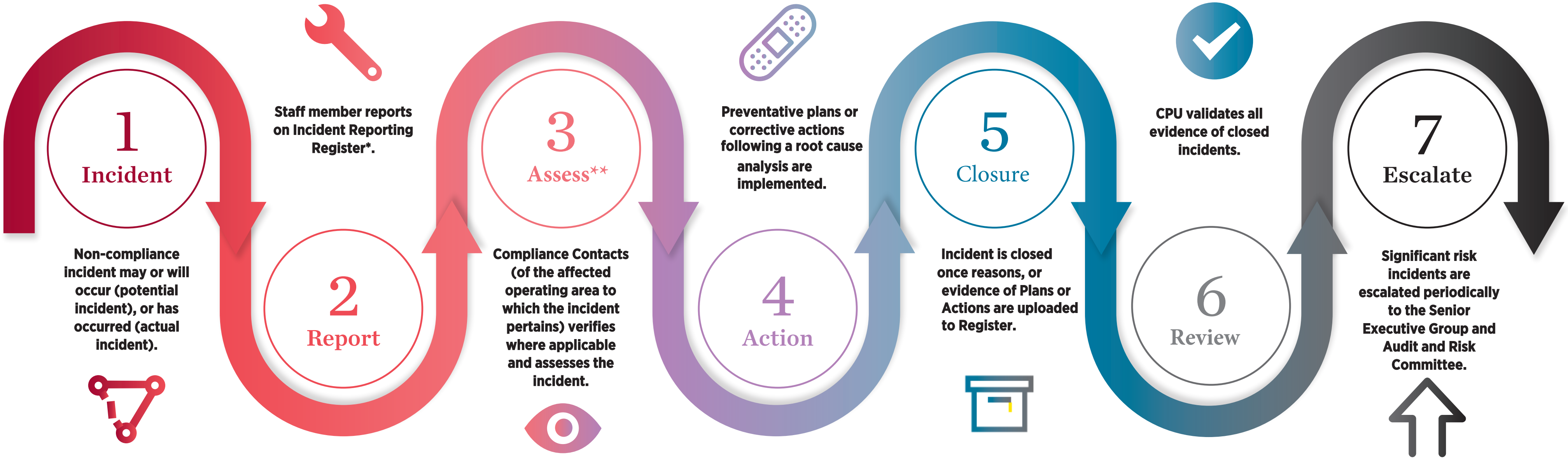
✋ General information about the Compliance Management Program is also mentioned in the Manager Training, and Staff Induction training by the Talent, Learning, and Development unit.

OTHER FACTSHEETS

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

WESTERN SYDNEY
UNIVERSITY

NON-COMPLIANCE INCIDENT REPORTING



1 Incident

Non-compliance incident may or will occur (potential incident), or has occurred (actual incident).

2 Report

Staff member reports on Incident Reporting Register*.

3 Assess**

Compliance Contacts (of the affected operating area to which the incident pertains) verifies where applicable and assesses the incident.

4 Action

Preventative plans or corrective actions following a root cause analysis are implemented.

5 Closure

Incident is closed once reasons, or evidence of Plans or Actions are uploaded to Register.

6 Review

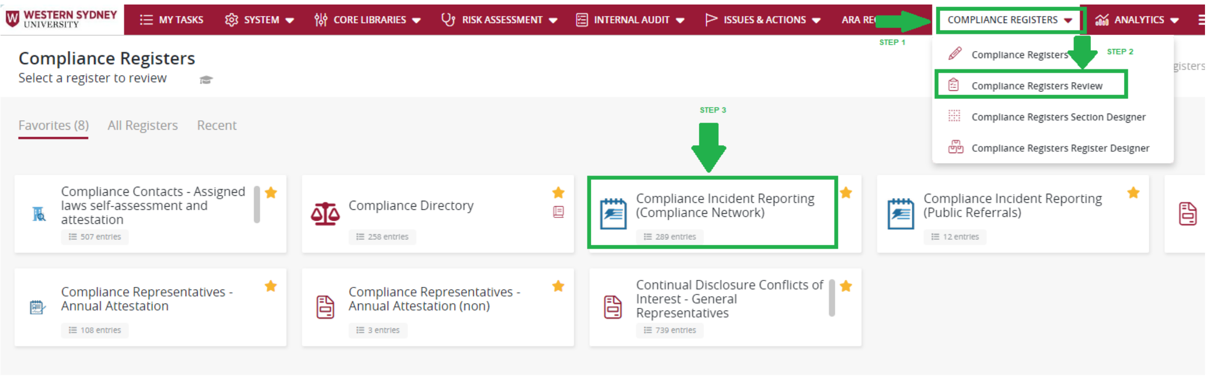
CPU validates all evidence of closed incidents.

7 Escalate

Significant risk incidents are escalated periodically to the Senior Executive Group and Audit and Risk Committee.

*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

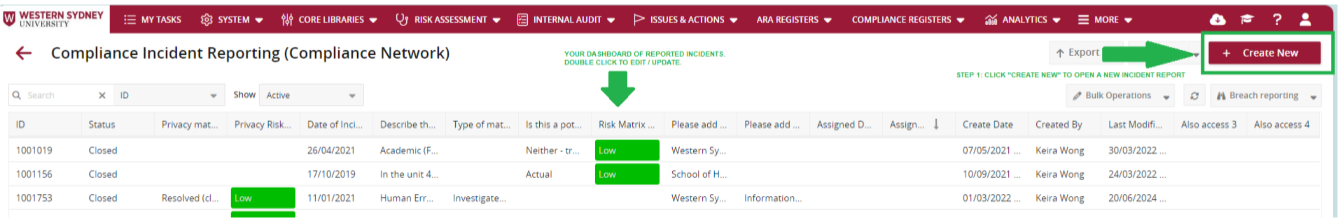


Compliance Registers

Select a register to review

Favorites (8) All Registers Recent

- Compliance Contacts - Assigned laws self-assessment and attestation — 507 entries
- Compliance Directory — 258 entries
- Compliance Incident Reporting (Compliance Network) — 289 entries
- Compliance Incident Reporting (Public Referrals) — 12 entries
- Compliance Representatives - Annual Attestation — 108 entries
- Compliance Representatives - Annual Attestation (non) — 3 entries
- Continual Disclosure Conflicts of Interest - General Representatives — 739 entries

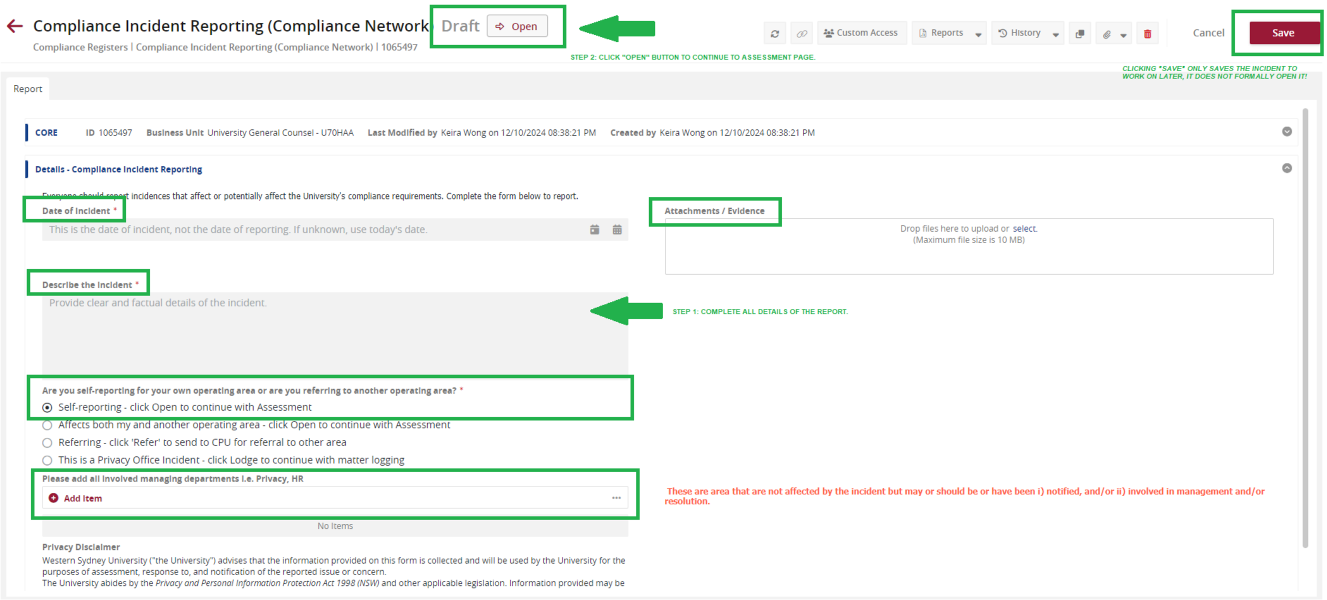


Compliance Incident Reporting (Compliance Network)

YOUR DASHBOARD OF REPORTED INCIDENTS. DOUBLE CLICK TO EDIT / UPDATE.

STEP 1: CLICK "CREATE NEW" TO OPEN A NEW INCIDENT REPORT

ID	Status	Privacy mat...	Privacy Risk...	Date of Inci...	Describe th...	Type of mat...	Is this a pot...	Risk Matrix ...	Please add ...	Please add ...	Assigned D...	Assign... ↓	Create Date	Created By	Last Modifi...	Also access 3	Also access 4
1001019	Closed			26/04/2021	Academic (F...		Neither - tr...	Low	Western Sy...				07/05/2021 ...	Keira Wong	30/03/2022 ...		
1001156	Closed			17/10/2019	In the unit 4...		Actual	Low	School of H...				10/09/2021 ...	Keira Wong	24/03/2022 ...		
1001753	Closed	Resolved (cl...	Low	11/01/2021	Human Err...	Investigate...			Western Sy...	Information...			01/03/2022 ...	Keira Wong	20/06/2024 ...		



Compliance Incident Reporting (Compliance Network) Draft

Compliance Registers | Compliance Incident Reporting (Compliance Network) | 1065497

STEP 2: CLICK "OPEN" BUTTON TO CONTINUE TO ASSESSMENT PAGE.

CLICKING "SAVE" ONLY SAVES THE INCIDENT TO WORK ON LATER, IT DOES NOT FORMALLY OPEN IT!

CORE **ID** 1065497 **Business Unit** University General Counsel - U70HAA **Last Modified by** Keira Wong on 12/10/2024 08:38:21 PM **Created by** Keira Wong on 12/10/2024 08:38:21 PM

Details - Compliance Incident Reporting

Everyone should report incidences that affect or potentially affect the University's compliance requirements. Complete the form below to report.

Date of Incident *

This is the date of incident, not the date of reporting. If unknown, use today's date.

Attachments / Evidence

Drop files here to upload or select.
(Maximum file size is 10 MB)

Describe the Incident *

Provide clear and factual details of the incident.

STEP 1: COMPLETE ALL DETAILS OF THE REPORT.

Are you self-reporting for your own operating area or are you referring to another operating area? *

● Self-reporting - click Open to continue with Assessment

○ Affects both my and another operating area - click Open to continue with Assessment

○ Referring - click 'Refer' to send to CPU for referral to other area

○ This is a Privacy Office Incident - click Lodge to continue with matter logging

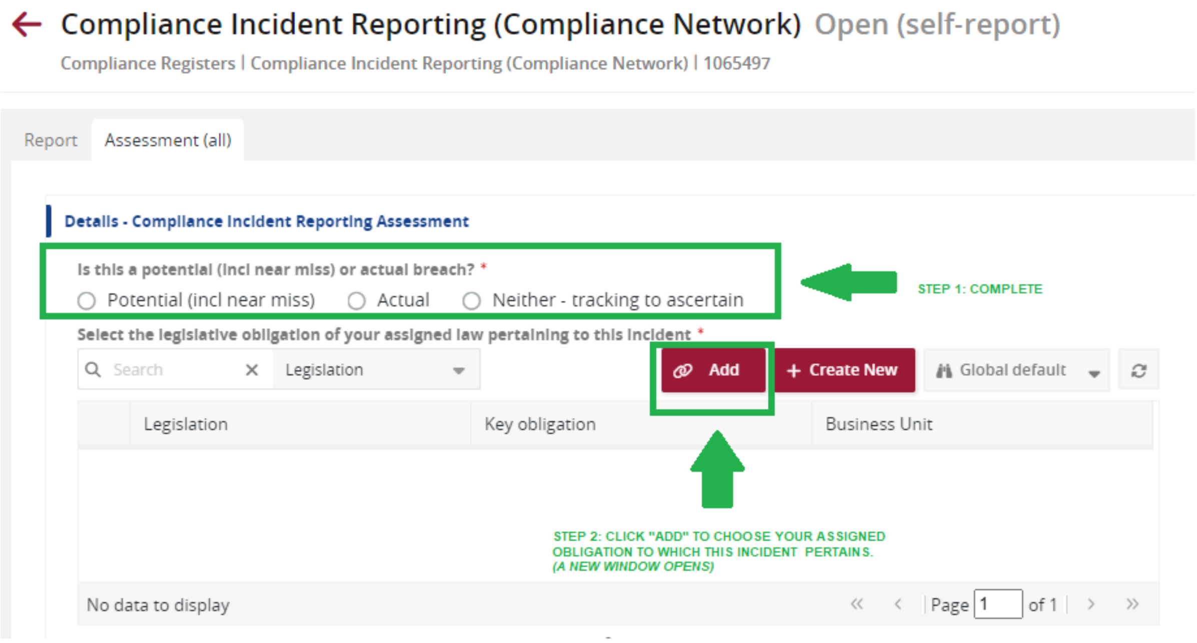
Please add all involved managing departments i.e. Privacy, HR

No Items

These are area that are not affected by the incident but may or should be or have been i) notified, and/or ii) involved in management and/or resolution.

Privacy Disclaimer

Western Sydney University ("the University") advises that the information provided on this form is collected and will be used by the University for the purposes of assessment, response to, and notification of the reported issue or concern.
The University abides by the *Privacy and Personal Information Protection Act 1998 (NSW)* and other applicable legislation. Information provided may be



Compliance Incident Reporting (Compliance Network) Open (self-report)

Compliance Registers | Compliance Incident Reporting (Compliance Network) | 1065497

Details - Compliance Incident Reporting Assessment

Is this a potential (incl near miss) or actual breach? *

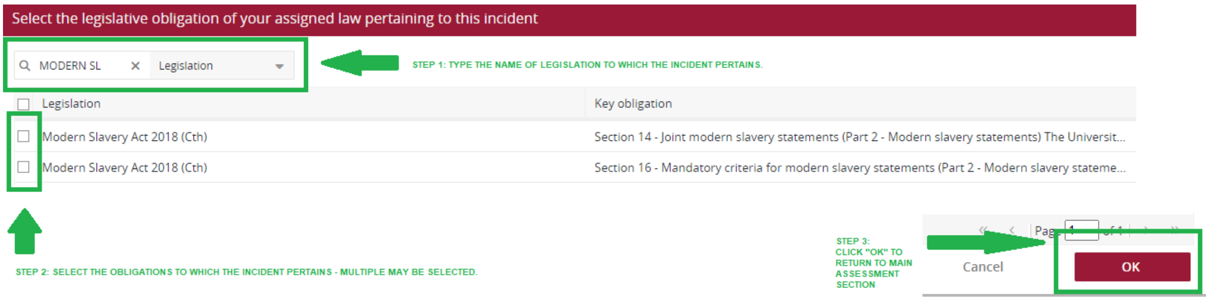
○ Potential (incl near miss) ○ Actual ○ Neither - tracking to ascertain

STEP 1: COMPLETE

Select the legislative obligation of your assigned law pertaining to this incident *

Legislation	Key obligation	Business Unit
No data to display		

STEP 2: CLICK "ADD" TO CHOOSE YOUR ASSIGNED OBLIGATION TO WHICH THIS INCIDENT PERTAINS.
(A NEW WINDOW OPENS)



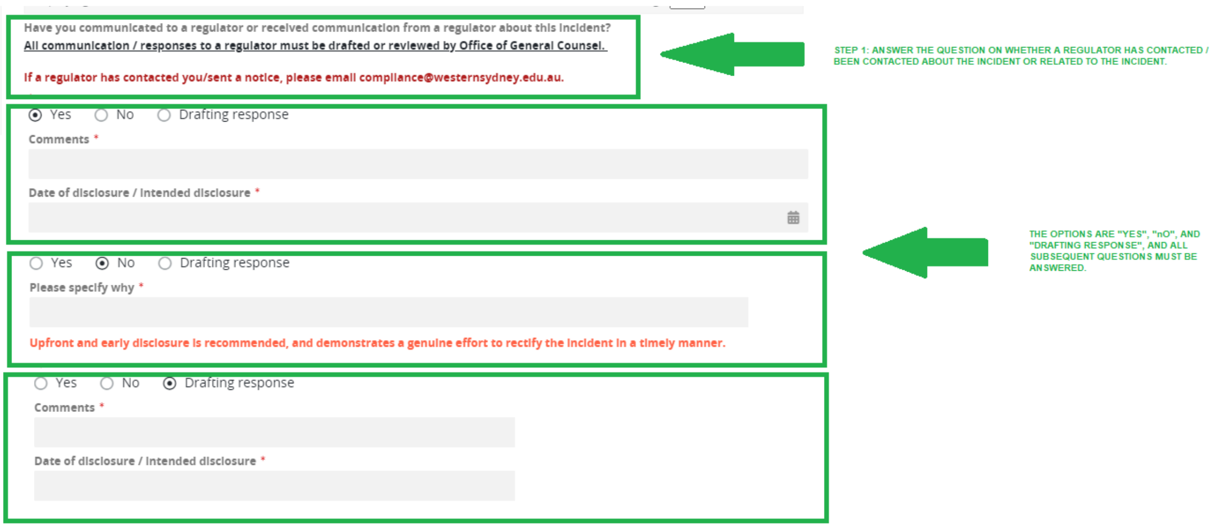
Select the legislative obligation of your assigned law pertaining to this incident

STEP 1: TYPE THE NAME OF LEGISLATION TO WHICH THE INCIDENT PERTAINS.

□ Legislation	Key obligation
□ Modern Slavery Act 2018 (Cth)	Section 14 - Joint modern slavery statements (Part 2 - Modern slavery statements) The Universit...
□ Modern Slavery Act 2018 (Cth)	Section 16 - Mandatory criteria for modern slavery statements (Part 2 - Modern slavery stateme...

STEP 2: SELECT THE OBLIGATIONS TO WHICH THE INCIDENT PERTAINS - MULTIPLE MAY BE SELECTED.

STEP 3:
CLICK "OK" TO RETURN TO MAIN ASSESSMENT SECTION



Have you communicated to a regulator or received communication from a regulator about this incident?

All communication / responses to a regulator must be drafted or reviewed by Office of General Counsel.

If a regulator has contacted you/sent a notice, please email compliance@westernsydney.edu.au.

STEP 1: ANSWER THE QUESTION ON WHETHER A REGULATOR HAS CONTACTED / BEEN CONTACTED ABOUT THE INCIDENT OR RELATED TO THE INCIDENT.

● Yes ○ No ○ Drafting response

Comments *

Date of disclosure / Intended disclosure *

○ Yes ● No ○ Drafting response

Please specify why *

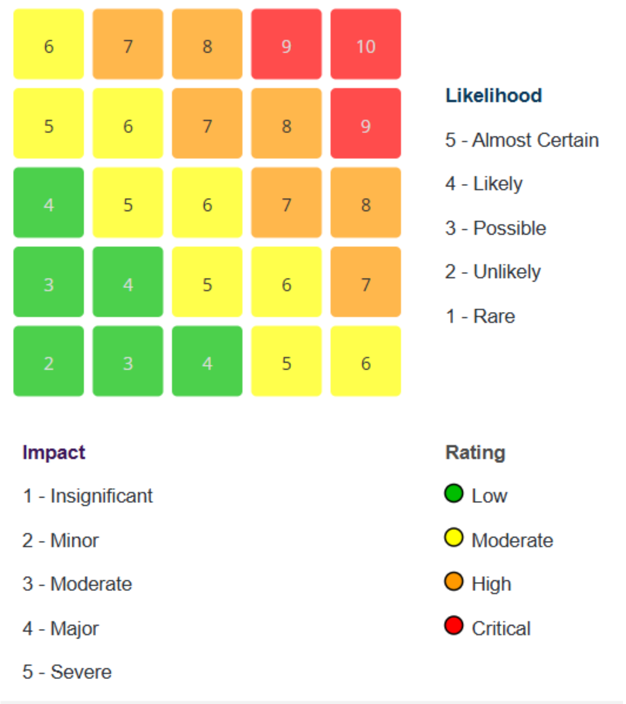
Upfront and early disclosure is recommended, and demonstrates a genuine effort to rectify the incident in a timely manner.

○ Yes ○ No ● Drafting response

Comments *

Date of disclosure / Intended disclosure *

THE OPTIONS ARE "YES", "nO", AND "DRAFTING RESPONSE", AND ALL SUBSEQUENT QUESTIONS MUST BE ANSWERED.



6	7	8	9	10
5	6	7	8	9
4	5	6	7	8
3	4	5	6	7
2	3	4	5	6

Likelihood

5 - Almost Certain

4 - Likely

3 - Possible

2 - Unlikely

1 - Rare

Impact

1 - Insignificant

2 - Minor

3 - Moderate

4 - Major

5 - Severe

Rating

🟢 Low

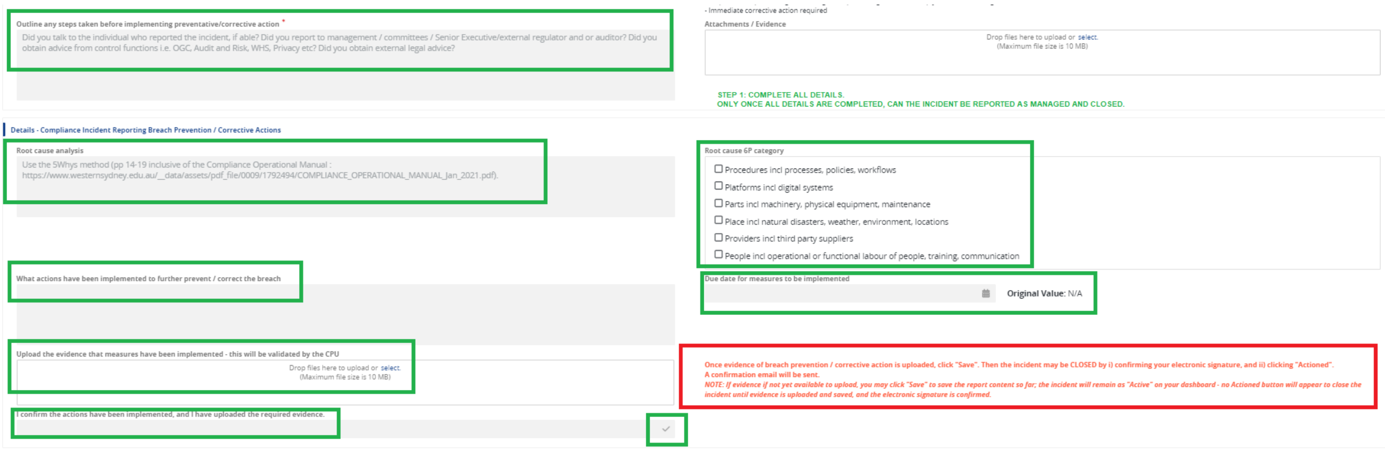
🟡 Moderate

🟠 High

🔴 Critical

STEP 1: ASSESS THE RISK RATING OF THE INCIDENT USING THE DEFINITIONS - LIKLIHOOD IS *ALWAYS* RATED AT '5' IF IT AN ACTUAL BREACH, '4' IF IT IS A NEAR MISS, '3' OR '4' IF POTENTIAL BREACH.

TRACKING INCIDENTS SHOULD BE ASSESSED AT LIKLIHOOD '3' OR '2' OR '1'.



Outline any steps taken before implementing preventative/corrective action *

Did you talk to the individual who reported the incident, if able? Did you report to management / committees / Senior Executive/external regulator and or auditor? Did you obtain advice from control functions i.e. OGC, Audit and Risk, WHS, Privacy etc? Did you obtain external legal advice?

- Immediate corrective action required

Attachments / Evidence

Drop files here to upload or select.
(Maximum file size is 10 MB)

STEP 1: COMPLETE ALL DETAILS.
ONLY ONCE ALL DETAILS ARE COMPLETED, CAN THE INCIDENT BE REPORTED AS MANAGED AND CLOSED.

Details - Compliance Incident Reporting Breach Prevention / Corrective Actions

Root cause analysis

Use the 5Whys method (pp 14-19 inclusive of the Compliance Operational Manual : https://www.westernsydney.edu.au/__data/assets/pdf_file/0009/1792494/COMPLIANCE_OPERATIONAL_MANUAL_Jan_2021.pdf).

Root cause 6P category

- ☐ Procedures incl processes, policies, workflows
- ☐ Platforms incl digital systems
- ☐ Parts incl machinery, physical equipment, maintenance
- ☐ Place incl natural disasters, weather, environment, locations
- ☐ Providers incl third party suppliers
- ☐ People incl operational or functional labour of people, training, communication

What actions have been implemented to further prevent / correct the breach

Due date for measures to be implemented

Original Value: N/A

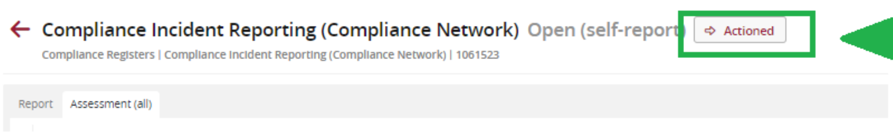
Upload the evidence that measures have been implemented - this will be validated by the CPU

Drop files here to upload or select.
(Maximum file size is 10 MB)

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.

I confirm the actions have been implemented, and I have uploaded the required evidence.

✓



Compliance Incident Reporting (Compliance Network) Open (self-report)

Compliance Registers | Compliance Incident Reporting (Compliance Network) | 1061523

STEP 1: CLICK "ACTIONED" ONCE ALL INFORMATION IS ENTERED TO MANAGE AND CLOSE THE INCIDENT.

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.

COMPLIANCE RISK ASSESSMENT MATRIX

Multiply the score of likelihood with the score of impact to ascertain final rating.

E.g. Unlikely likelihood (2) multiplied by Moderate impact (3) = 6 in yellow square = Moderate rating

🟨 6	🟧 7	🟧 8	🟥 9	🟥 10
🟨 5	🟨 6	🟧 7	🟧 8	🟥 9
🟩 4	🟨 5	🟨 6	🟧 7	🟧 8
🟩 3	🟩 4	🟨 5	🟨 6	🟧 7
🟩 2	🟩 3	🟩 4	🟨 5	🟨 6

Likelihood

5 - Almost Certain

4 - Likely

3 - Possible

2 - Unlikely

1 - Rare

Impact

1 - Insignificant

2 - Minor

3 - Moderate

4 - Major

5 - Severe

Rating

🟢 Low

🟡 Moderate

🟠 High

🔴 Critical

The following definitions and thresholds should be used when rating the breaches.

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 *(No formal action plan required. Should be monitored at the local level using business-as-usual procedures and internal controls. No further mitigation necessary unless risk conditions change.)*:
- Minor non-compliances or breaches of contract, Act, regulations, consent conditions
- Minor regulatory scrutiny via improvement letters

(3) Moderate *(Action required within six months that requires active monitoring.)*:
- Breach of contract, Act, regulation, or consent conditions
- Potential for allegations of criminal/unlawful conduct
- Individual liability
- Regulator infringement notices
- Corrective action managed locally

(4) Major *(Action required within three months. Mitigation measures should be implemented promptly to reduce risk exposure.)*:
- Major breach of contract/Act/regulations/consent conditions
- Investigation, prosecution, or major fines possible
- Potential for litigation
- Allegations of criminal/unlawful conduct
- Senior Executive liability
- Expected to attract regulatory attention / Required to report to regulator / Regulatory audits / Warning letters
- Short term corrective action required and demonstrably managed via action plan

(5) Catastrophic *(Immediate attention required. Urgent mitigation measures must be implemented without delay.)*:
- Serious breach of legislation/contract with significant prosecution (including imprisonment)/fines likely
- Future funding/approvals/registration/licensing in jeopardy
- Potential litigation including class actions and damages and/or costs awarded
- Criminal or civil proceedings initiated
- Board liability
- Required to report to regulator / Regulator publishing failure to comply with notices / Regulator sanctions
- Immediate corrective action required

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".

Compliance Management Program Annual Attestation Process Document

EMAIL SENT IN OCTOBER:

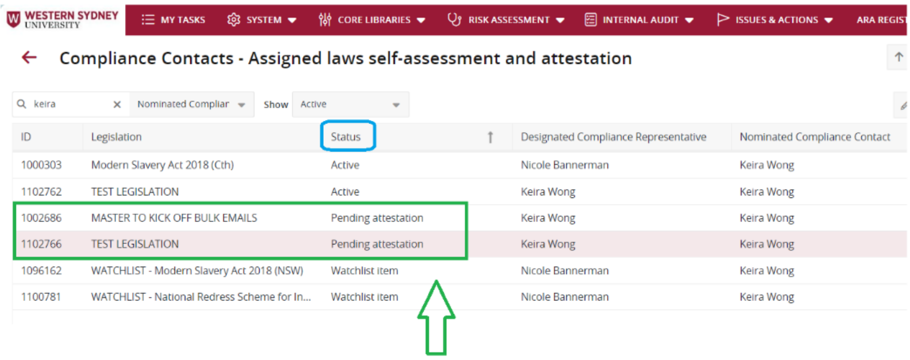
Compliance Program Unit (CPU) sends an email to the Nominated Compliance Contact with a link to the dashboard of all their assigned laws, instructing to complete the annual attestation for each assigned law.

COMPLETE ATTESTATION BETWEEN OCTOBER START TO NOVEMBER END

A. 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.



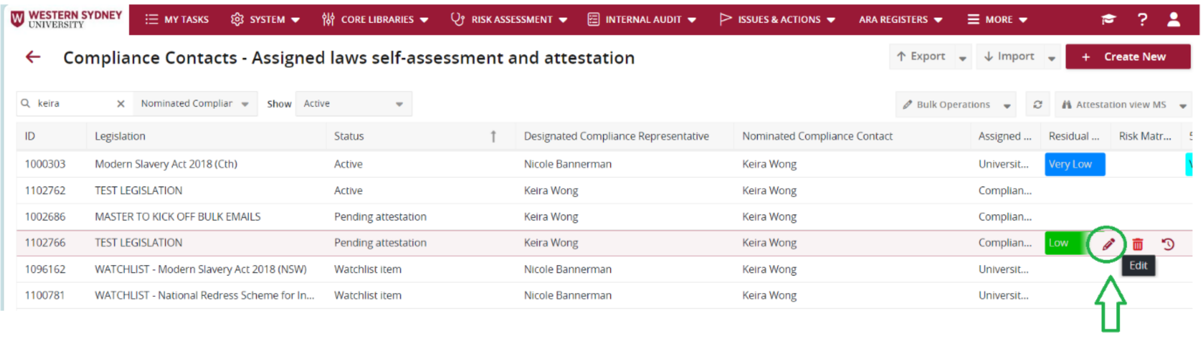
Compliance Contacts - Assigned laws self-assessment and attestation

keira | Nominated Compliar | Show Active

ID	Legislation	Status	Designated Compliance Representative	Nominated Compliance Contact
1000303	Modern Slavery Act 2018 (Cth)	Active	Nicole Bannerman	Keira Wong
1102762	TEST LEGISLATION	Active	Keira Wong	Keira Wong
1002686	MASTER TO KICK OFF BULK EMAILS	Pending attestation	Keira Wong	Keira Wong
1102766	TEST LEGISLATION	Pending attestation	Keira Wong	Keira Wong
1096162	WATCHLIST - Modern Slavery Act 2018 (NSW)	Watchlist item	Nicole Bannerman	Keira Wong
1100781	WATCHLIST - National Redress Scheme for In...	Watchlist item	Nicole Bannerman	Keira Wong

Only those tagged as "Pending Attestation" need to be attested to

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



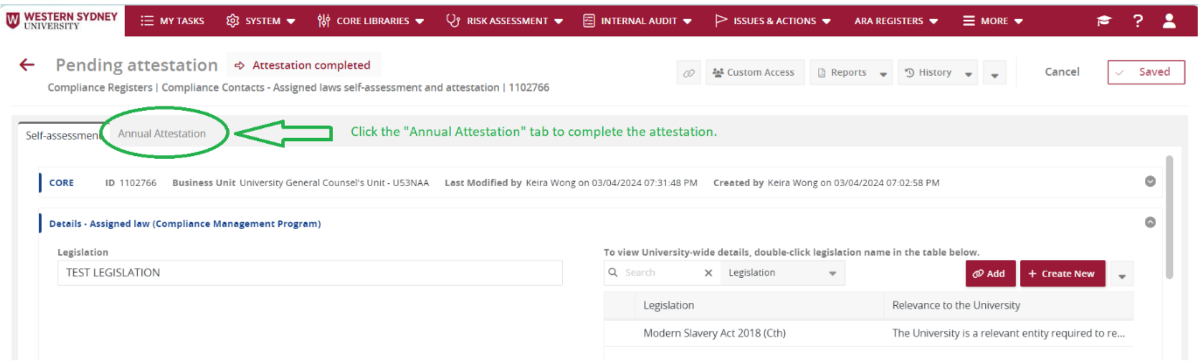
Compliance Contacts - Assigned laws self-assessment and attestation

keira | Nominated Compliar | Show Active

ID	Legislation	Status	Designated Compliance Representative	Nominated Compliance Contact	Assigned ...	Residual ...	Risk Matr...
1000303	Modern Slavery Act 2018 (Cth)	Active	Nicole Bannerman	Keira Wong	Universit...	Very Low	
1102762	TEST LEGISLATION	Active	Keira Wong	Keira Wong	Complian...		
1002686	MASTER TO KICK OFF BULK EMAILS	Pending attestation	Keira Wong	Keira Wong	Complian...		
1102766	TEST LEGISLATION	Pending attestation	Keira Wong	Keira Wong	Complian...	Low	
1096162	WATCHLIST - Modern Slavery Act 2018 (NSW)	Watchlist item	Nicole Bannerman	Keira Wong	Universit...		
1100781	WATCHLIST - National Redress Scheme for In...	Watchlist item	Nicole Bannerman	Keira Wong	Universit...		

Click the pencil icon to edit the assigned item to complete the attestation

C. Toggle to “Annual Attestation” tab.



Pending attestation
Attestation completed
Compliance Registers | Compliance Contacts - Assigned laws self-assessment and attestation | 1102766

Click the "Annual Attestation" tab to complete the attestation.

CORE ID 1102766 **Business Unit** University General Counsel's Unit - U53NAA **Last Modified by** Keira Wong on 03/04/2024 07:31:48 PM **Created by** Keira Wong on 03/04/2024 07:02:58 PM

Details - Assigned law (Compliance Management Program)

Legislation: TEST LEGISLATION

To view University-wide details, double-click legislation name in the table below.

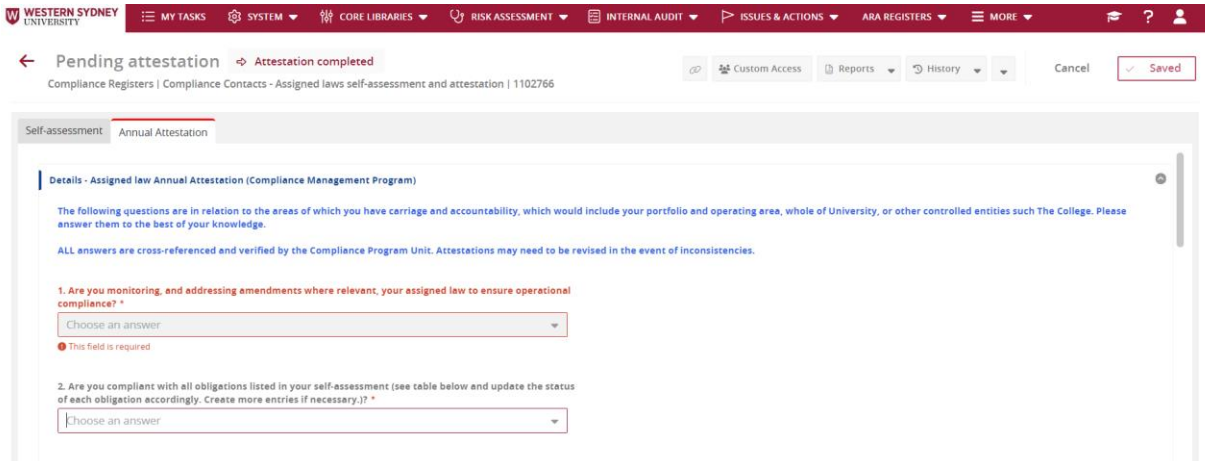
Search: Legislation

Legislation	Relevance to the University
Modern Slavery Act 2018 (Cth)	The University is a relevant entity required to re...

D. 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.



Pending attestation
Attestation completed
Compliance Registers | Compliance Contacts - Assigned laws self-assessment and attestation | 1102766

Details - Assigned law Annual Attestation (Compliance Management Program)

The following questions are in relation to the areas of which you have carriage and accountability, which would include your portfolio and operating area, whole of University, or other controlled entities such The College. Please answer them to the best of your knowledge.

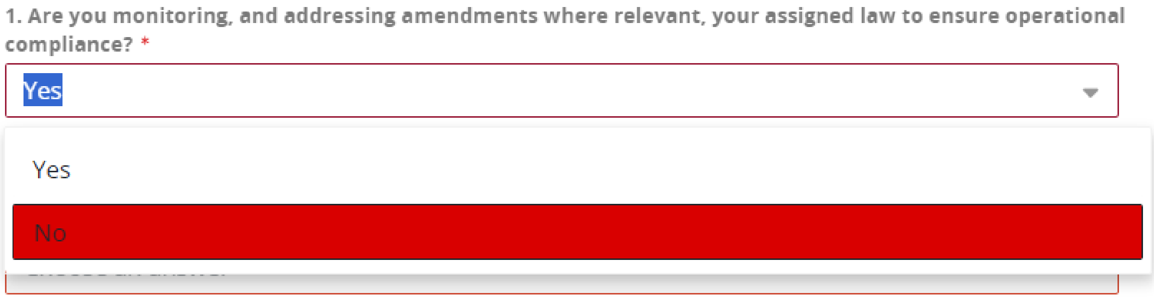
ALL answers are cross-referenced and verified by the Compliance Program Unit. Attestations may need to be revised in the event of inconsistencies.

1. Are you monitoring, and addressing amendments where relevant, your assigned law to ensure operational compliance? *
Choose an answer
This field is required

2. Are you compliant with all obligations listed in your self-assessment (see table below and update the status of each obligation accordingly. Create more entries if necessary.)? *
Choose an answer

Here is a guide to the questions:

Question 1.



1. Are you monitoring, and addressing amendments where relevant, your assigned law to ensure operational compliance? *

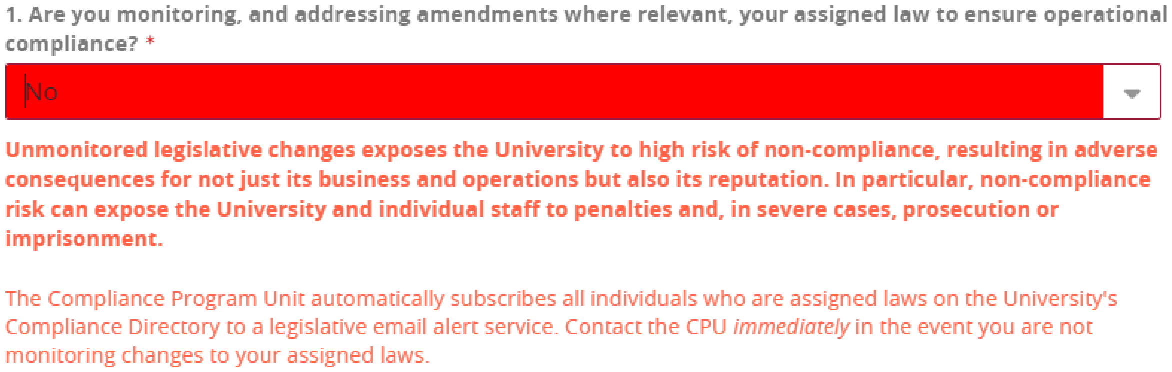
Yes

Yes

No

- 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.



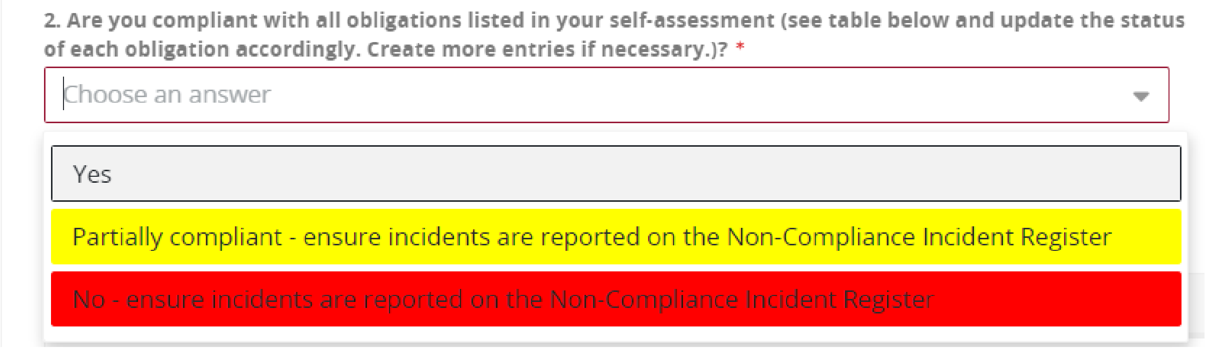
1. Are you monitoring, and addressing amendments where relevant, your assigned law to ensure operational compliance? *

No

Unmonitored legislative changes exposes the University to high risk of non-compliance, resulting in adverse consequences for not just its business and operations but also its reputation. In particular, non-compliance risk can expose the University and individual staff to penalties and, in severe cases, prosecution or imprisonment.

The Compliance Program Unit automatically subscribes all individuals who are assigned laws on the University's Compliance Directory to a legislative email alert service. Contact the CPU *immediately* in the event you are not monitoring changes to your assigned laws.

Question 2.



2. Are you compliant with all obligations listed in your self-assessment (see table below and update the status of each obligation accordingly. Create more entries if necessary.)? *

Choose an answer

Yes

Partially compliant - ensure incidents are reported on the Non-Compliance Incident Register

No - ensure incidents are reported on the Non-Compliance Incident Register

- 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 2A.

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

i) the obligation (if needed)

ii) compliance status from “Unknown”

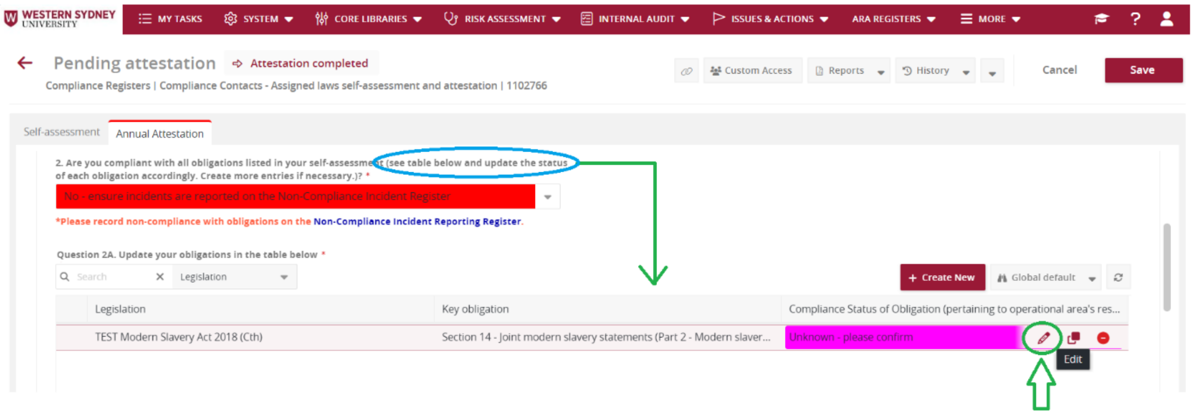
iii) statement of evidence of compliance

iv) attachment of evidence if able

v) controls that mitigate the non-compliance risk, adding more or deleting, as long as it is current and accurate (do not enter controls that aren’t yet executed)

vi) statement of evidence of controls

vii) attachment of evidence if able



Pending attestation — Attestation completed

Compliance Registers | Compliance Contacts - Assigned laws self-assessment and attestation | 1102766

2. Are you compliant with all obligations listed in your self-assessment (see table below and update the status of each obligation accordingly. Create more entries if necessary.)? *

No - ensure incidents are reported on the Non-Compliance Incident Register

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

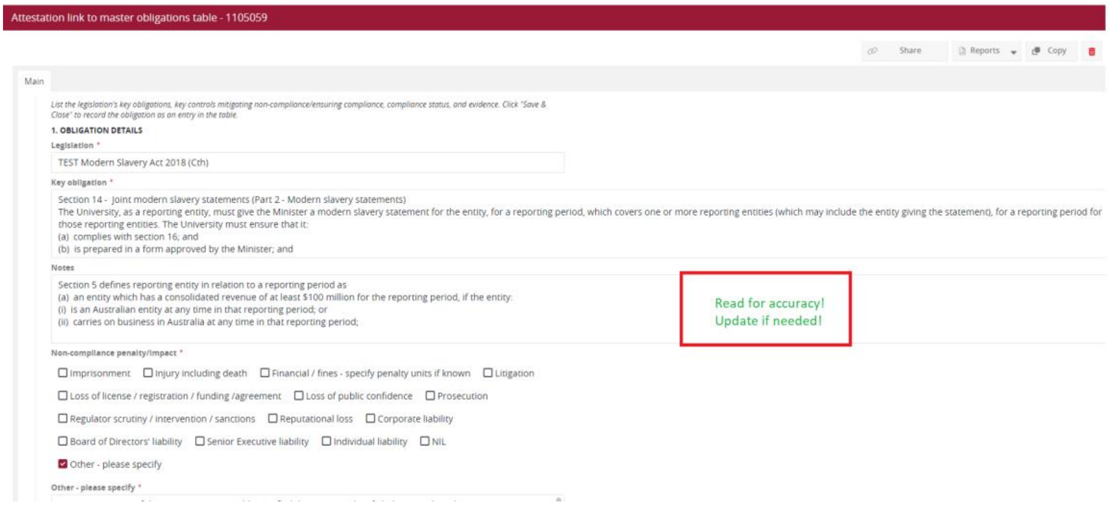
Question 2A. Update your obligations in the table below *

Search — Legislation

Legislation	Key obligation	Compliance Status of Obligation (pertaining to operational area's res...
TEST Modern Slavery Act 2018 (Cth)	Section 14 - Joint modern slavery statements (Part 2 - Modern slaver...	Unknown - please confirm

Click the pencil icon to update the compliance status and controls, and to provide evidence if able.

i) Read and update the the obligation (if needed).



Attestation link to master obligations table - 1105059

List the legislation's key obligations, key controls mitigating non-compliance/ensuring compliance, compliance status, and evidence. Click "Save & Close" to record the obligation as an entry in the table.

1. OBLIGATION DETAILS

Legislation *

TEST Modern Slavery Act 2018 (Cth)

Key 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

Notes

Section 5 defines reporting entity in relation to a reporting period as
(a) an entity which has a consolidated revenue of at least $100 million for the reporting period, if the entity:
(i) is an Australian entity at any time in that reporting period; or
(ii) carries on business in Australia at any time in that reporting period;

Read for accuracy!
Update if needed!

Non-compliance penalty/impact *

□ Imprisonment □ Injury including death □ Financial / fines - specify penalty units if known □ Litigation

□ Loss of license / registration / funding /agreement □ Loss of public confidence □ Prosecution

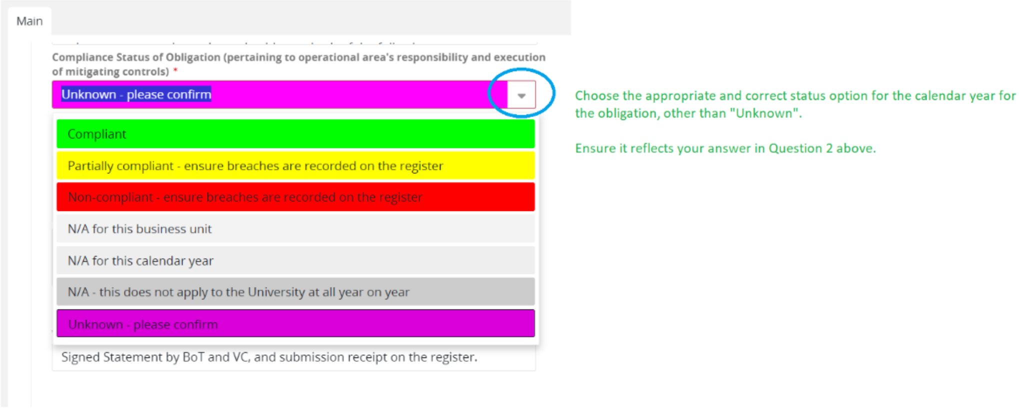
□ Regulator scrutiny / intervention / sanctions □ Reputational loss □ Corporate liability

□ Board of Directors' liability □ Senior Executive liability □ Individual liability □ NIL

☑ Other - please specify

Other - please specify *

ii) Update the compliance status from “Unknown”



Main

Compliance Status of Obligation (pertaining to operational area's responsibility and execution of mitigating controls) *

Unknown - please confirm

- Compliant
- Partially compliant - ensure breaches are recorded on the register
- Non-compliant - ensure breaches are recorded on the register
- N/A for this business unit
- N/A for this calendar year
- N/A - this does not apply to the University at all year on year
- Unknown - please confirm

Signed Statement by BoT and VC, and submission receipt on the register.

Choose the appropriate and correct status option for the calendar year for the obligation, other than "Unknown".

Ensure it reflects your answer in Question 2 above.

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”.

Note: Fields iii) and iv) are not required if the status is marked “N/A…”

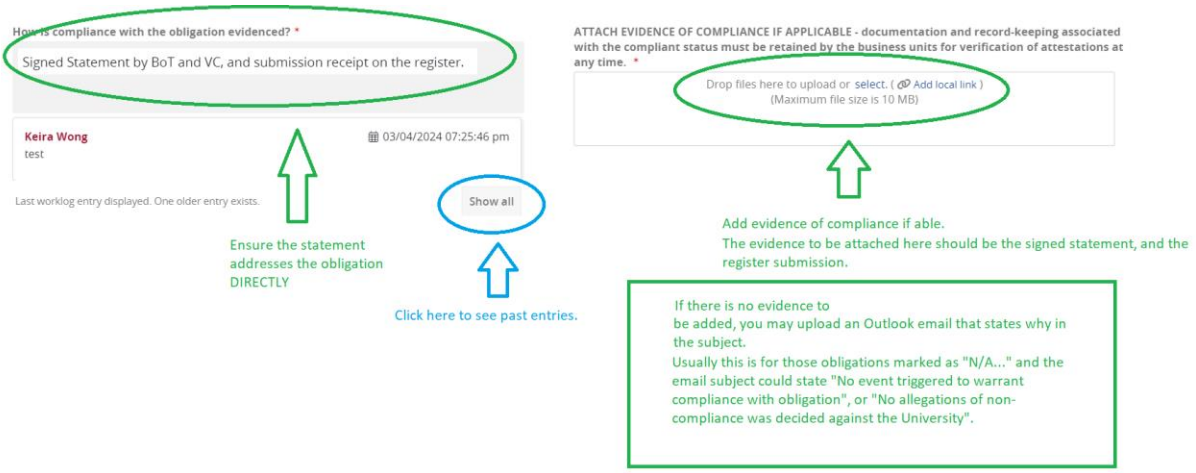
iii) Update the statement of evidence of compliance

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”.

iv) Update the attachment of evidence if able

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.



How is compliance with the obligation evidenced? *

Signed Statement by BoT and VC, and submission receipt on the register.

Keira Wong 03/04/2024 07:25:46 pm
test

Last worklog entry displayed. One older entry exists.

Ensure the statement addresses the obligation DIRECTLY

Click here to see past entries.

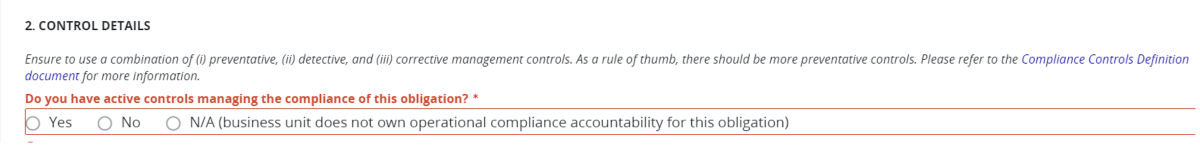
ATTACH EVIDENCE OF COMPLIANCE IF APPLICABLE - documentation and record-keeping associated with the compliant status must be retained by the business units for verification of attestations at any time. *

Drop files here to upload or select. (Add local link)
(Maximum file size is 10 MB)

Add evidence of compliance if able.
The evidence to be attached here should be the signed statement, and the register submission.

If there is no evidence to be added, you may upload an Outlook email that states why in the subject.
Usually this is for those obligations marked as "N/A..." and the email subject could state "No event triggered to warrant compliance with obligation", or "No allegations of non-compliance was decided against the University".

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



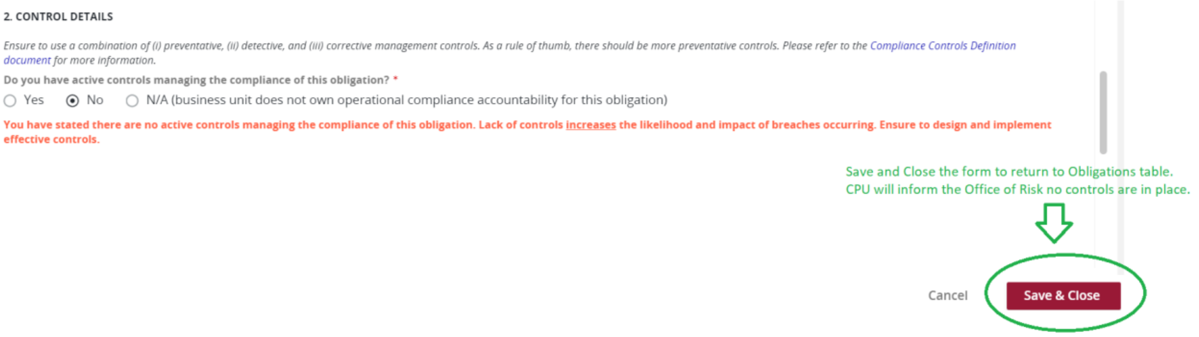
2. CONTROL DETAILS

Ensure to use a combination of (i) preventative, (ii) detective, and (iii) corrective management controls. As a rule of thumb, there should be more preventative controls. Please refer to the Compliance Controls Definition document for more information.

Do you have active controls managing the compliance of this obligation? *

○ Yes ○ No ○ N/A (business unit does not own operational compliance accountability for this obligation)

- 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.



2. CONTROL DETAILS

Ensure to use a combination of (i) preventative, (ii) detective, and (iii) corrective management controls. As a rule of thumb, there should be more preventative controls. Please refer to the Compliance Controls Definition document for more information.

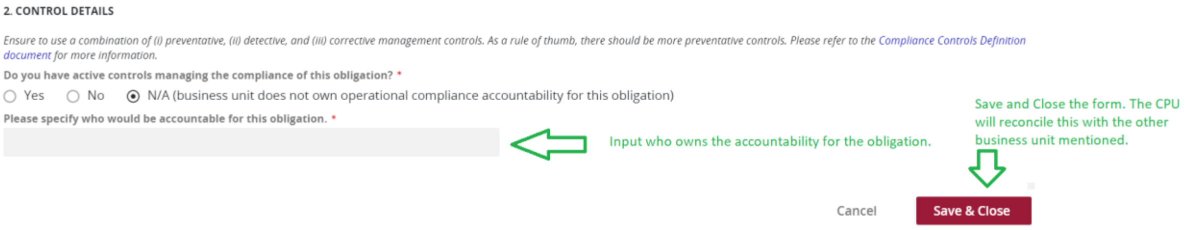
Do you have active controls managing the compliance of this obligation? *

○ Yes ● No ○ N/A (business unit does not own operational compliance accountability for this obligation)

You have stated there are no active controls managing the compliance of this obligation. Lack of controls increases the likelihood and impact of breaches occurring. Ensure to design and implement effective controls.

Save and Close the form to return to Obligations table.
CPU will inform the Office of Risk no controls are in place.

- 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.



2. CONTROL DETAILS

Ensure to use a combination of (i) preventative, (ii) detective, and (iii) corrective management controls. As a rule of thumb, there should be more preventative controls. Please refer to the Compliance Controls Definition document for more information.

Do you have active controls managing the compliance of this obligation? *

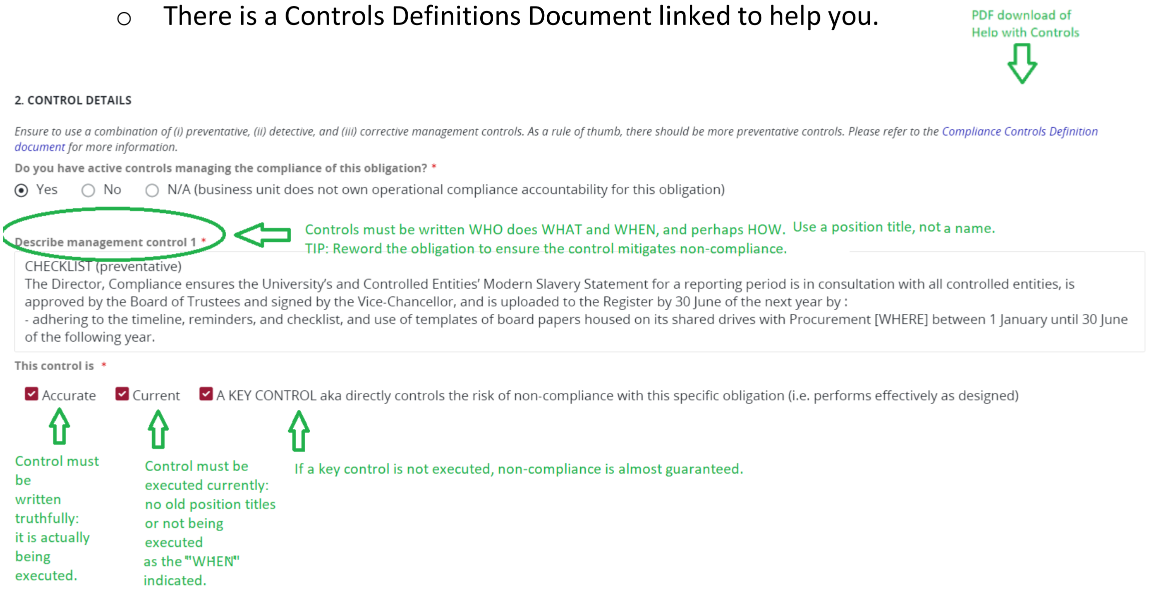
○ Yes ○ No ● N/A (business unit does not own operational compliance accountability for this obligation)

Please specify who would be accountable for this obligation. *

Input who owns the accountability for the obligation.

Save and Close the form. The CPU will reconcile this with the other business unit mentioned.

- 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.
  - There is a Controls Definitions Document linked to help you.



PDF download of Help with Controls

2. CONTROL DETAILS

Ensure to use a combination of (i) preventative, (ii) detective, and (iii) corrective management controls. As a rule of thumb, there should be more preventative controls. Please refer to the Compliance Controls Definition document for more information.

Do you have active controls managing the compliance of this obligation? *

● Yes ○ No ○ N/A (business unit does not own operational compliance accountability for this obligation)

Describe management control 1 *

Controls must be written WHO does WHAT and WHEN, and perhaps HOW. Use a position title, not a name.
TIP: Reword the obligation to ensure the control mitigates non-compliance.

CHECKLIST (preventative)
The Director, Compliance 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 by :
- adhering to the timeline, reminders, and checklist, and use of templates of board papers housed on its shared drives with Procurement [WHERE] between 1 January until 30 June of the following year.

This control is *

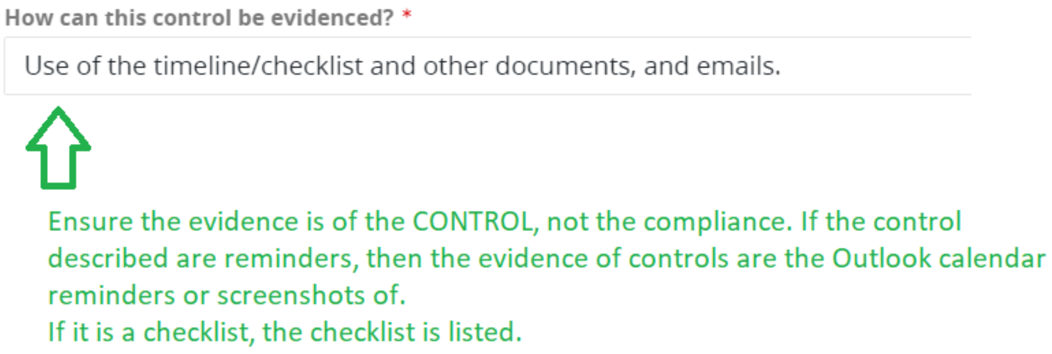
☑ Accurate ☑ Current ☑ A KEY CONTROL aka directly controls the risk of non-compliance with this specific obligation (i.e. performs effectively as designed)

Control must be written truthfully: it is actually being executed.

Control must be executed currently: no old position titles or not being executed as the "WHEN" indicated.

If a key control is not executed, non-compliance is almost guaranteed.

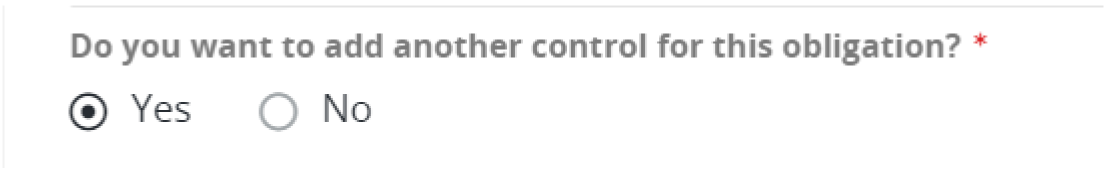
vi) Update the statement of evidence of controls



How can this control be evidenced? *

Use of the timeline/checklist and other documents, and emails.

Ensure the evidence is of the CONTROL, not the compliance. If the control described are reminders, then the evidence of controls are the Outlook calendar reminders or screenshots of.
If it is a checklist, the checklist is listed.



Do you want to add another control for this obligation? *

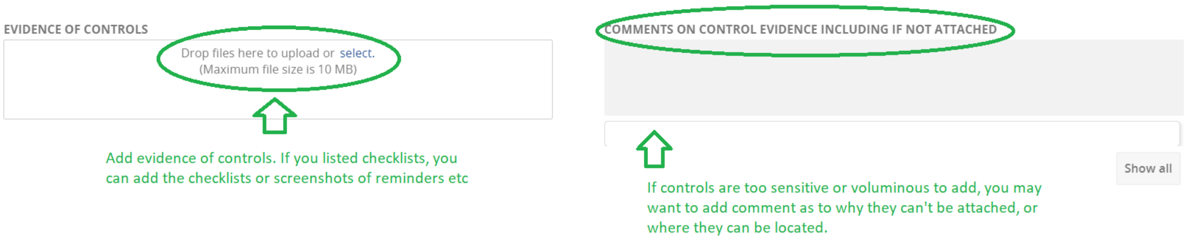
● Yes ○ No

- 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.

vii) Update the attachment of evidence of controls if able, or comment



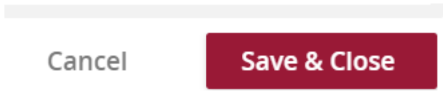
EVIDENCE OF CONTROLS

Drop files here to upload or select.
(Maximum file size is 10 MB)

Add evidence of controls. If you listed checklists, you can add the checklists or screenshots of reminders etc

COMMENTS ON CONTROL EVIDENCE INCLUDING IF NOT ATTACHED

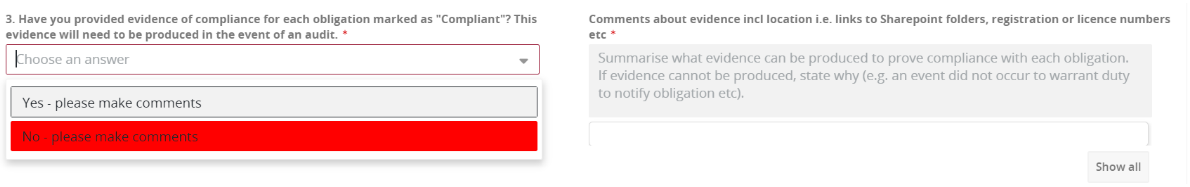
If controls are too sensitive or voluminous to add, you may want to add comment as to why they can't be attached, or where they can be located.



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

- **REPEAT FOR ALL LISTED OBLIGATIONS IN THE TABLE.**

Question 3.



3. Have you provided evidence of compliance for each obligation marked as "Compliant"? This evidence will need to be produced in the event of an audit. *

Choose an answer

- Yes - please make comments
- No - please make comments

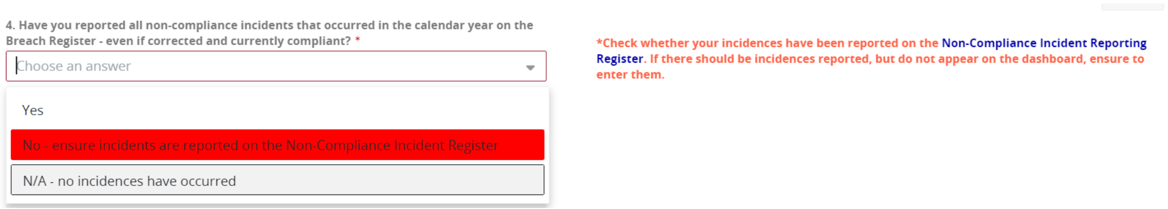
Comments about evidence incl location i.e. links to Sharepoint folders, registration or licence numbers etc *

Summarise what evidence can be produced to prove compliance with each obligation. If evidence cannot be produced, state why (e.g. an event did not occur to warrant duty to notify obligation etc).

- 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 4.



4. Have you reported all non-compliance incidents that occurred in the calendar year on the Breach Register - even if corrected and currently compliant? *

Choose an answer

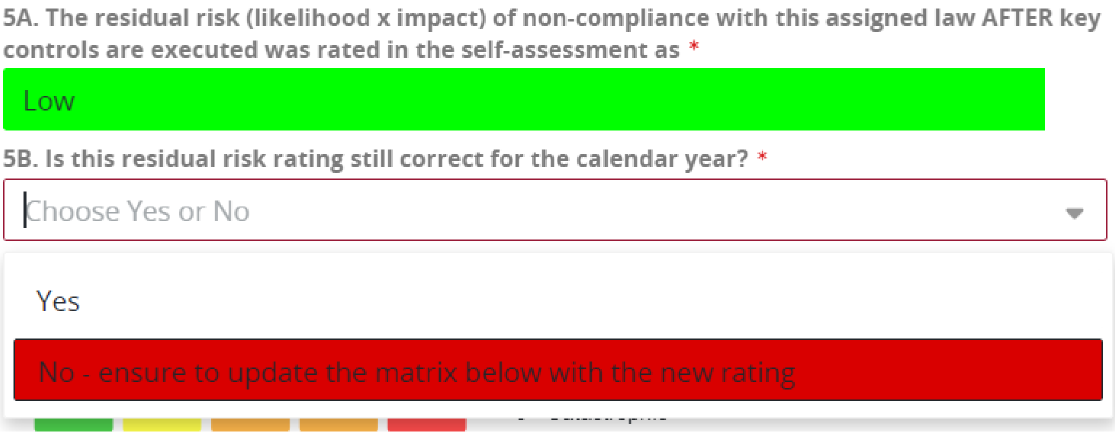
- Yes
- No - ensure incidents are reported on the Non-Compliance Incident Register
- N/A - no incidences have occurred

*Check whether your incidences have been reported on the Non-Compliance Incident Reporting Register. If there should be incidences reported, but do not appear on the dashboard, ensure to enter them.

- 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.

<u>Question 5.</u>



5A. The residual risk (likelihood x impact) of non-compliance with this assigned law AFTER key controls are executed was rated in the self-assessment as *

Low

5B. Is this residual risk rating still correct for the calendar year? *

Choose Yes or No

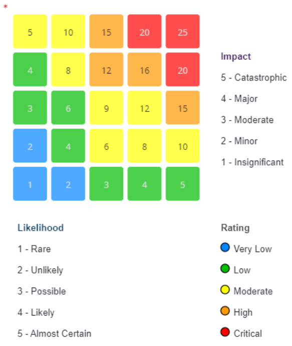
Yes

No - ensure to update the matrix below with the new rating

- 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).

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



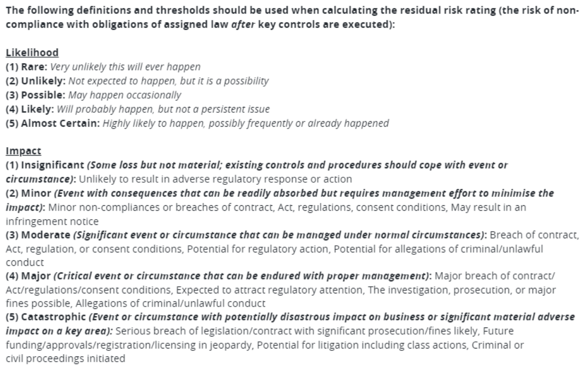
*

5	10	15	20	25
4	8	12	16	20
3	6	9	12	15
2	4	6	8	10
1	2	3	4	5

Impact
5 - Catastrophic
4 - Major
3 - Moderate
2 - Minor
1 - Insignificant

Likelihood
1 - Rare
2 - Unlikely
3 - Possible
4 - Likely
5 - Almost Certain

Rating
🔵 Very Low
🟢 Low
🟡 Moderate
🟠 High
🔴 Critical

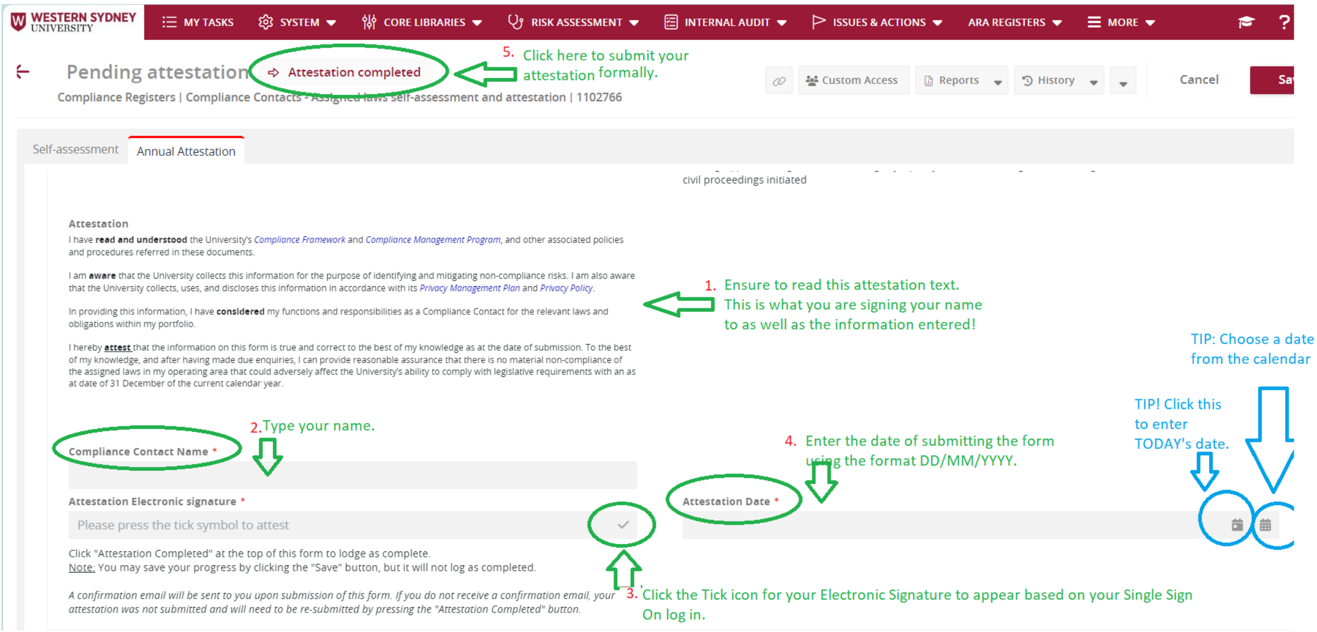


The following definitions and thresholds should be used when calculating the residual risk rating (the risk of non-compliance with obligations of assigned law *after* key controls are executed):

<u>**Likelihood**</u>
(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*

<u>**Impact**</u>
(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

E. COMPLETE AND SUBMIT YOUR ATTESTATION



Pending attestation

Compliance Registers | Compliance Contacts - Assigned laws self-assessment and attestation | 1102766

civil proceedings initiated

Attestation

I have **read and understood** the University's *Compliance Framework* and *Compliance Management Program*, and other associated policies and procedures referred in these documents.

I am **aware** that the University collects this information for the purpose of identifying and mitigating non-compliance risks. I am also aware that the University collects, uses, and discloses this information in accordance with its *Privacy Management Plan* and *Privacy Policy*.

In providing this information, I have **considered** my functions and responsibilities as a Compliance Contact for the relevant laws and obligations within my portfolio.

I hereby **attest** that the information on this form is true and correct to the best of my knowledge as at the date of submission. To the best of my knowledge, and after having made due enquiries, I can provide reasonable assurance that there is no material non-compliance of the assigned laws in my operating area that could adversely affect the University's ability to comply with legislative requirements with an as at date of 31 December of the current calendar year.

Compliance Contact Name *

Attestation Electronic signature *

Please press the tick symbol to attest ✓

Click "Attestation Completed" at the top of this form to lodge as complete.
Note: You may save your progress by clicking the "Save" button, but it will not log as completed.

A confirmation email will be sent to you upon submission of this form. If you do not receive a confirmation email, your attestation was not submitted and will need to be re-submitted by pressing the "Attestation Completed" button.

Attestation Date *

5. Click here to submit your attestation formally.

1. Ensure to read this attestation text. This is what you are signing your name to as well as the information entered!

TIP: Choose a date from the calendar

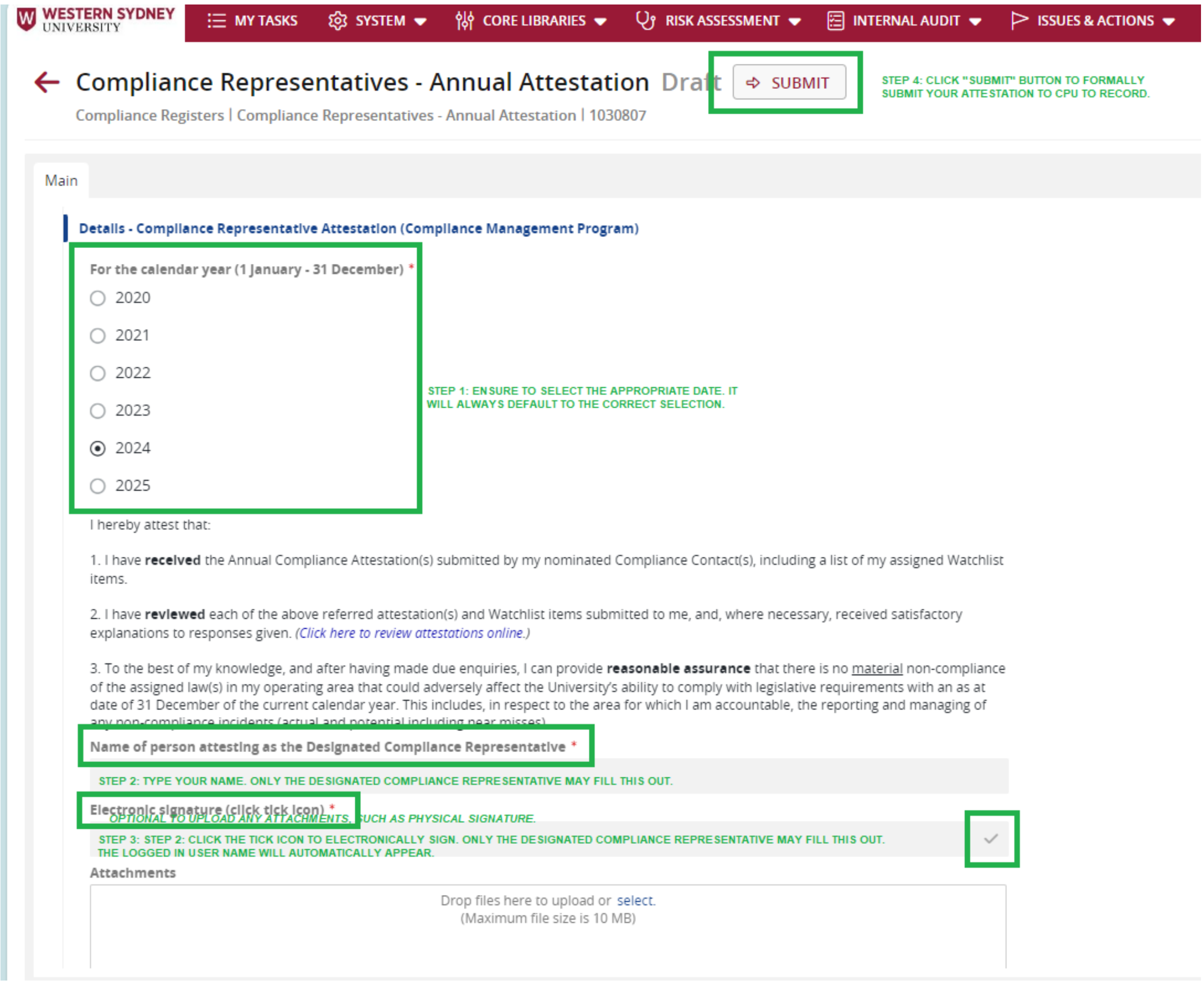
TIP! Click this to enter TODAY's date.

2. Type your name.

4. Enter the date of submitting the form using the format DD/MM/YYYY.

3. Click the Tick icon for your Electronic Signature to appear based on your Single Sign On log in.

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.**



Compliance Representatives - Annual Attestation Draft

Compliance Registers | Compliance Representatives - Annual Attestation | 1030807

STEP 4: CLICK "SUBMIT" BUTTON TO FORMALLY SUBMIT YOUR ATTESTATION TO CPU TO RECORD.

Details - Compliance Representative Attestation (Compliance Management Program)

For the calendar year (1 January - 31 December) *

○ 2020
○ 2021
○ 2022
○ 2023
● 2024
○ 2025

STEP 1: ENSURE TO SELECT THE APPROPRIATE DATE. IT WILL ALWAYS DEFAULT TO THE CORRECT SELECTION.

I hereby attest that:

1. I have **received** the Annual Compliance Attestation(s) submitted by my nominated Compliance Contact(s), including a list of my assigned Watchlist items.

2. I have **reviewed** each of the above referred attestation(s) and Watchlist items submitted to me, and, where necessary, received satisfactory explanations to responses given. *(Click here to review attestations online.)*

3. To the best of my knowledge, and after having made due enquiries, I can provide **reasonable assurance** that there is no material non-compliance of the assigned law(s) in my operating area that could adversely affect the University's ability to comply with legislative requirements with an as at date of 31 December of the current calendar year. This includes, in respect to the area for which I am accountable, the reporting and managing of any non-compliance incidents (actual and potential including near misses)

Name of person attesting as the Designated Compliance Representative *

STEP 2: TYPE YOUR NAME. ONLY THE DESIGNATED COMPLIANCE REPRESENTATIVE MAY FILL THIS OUT.

Electronic signature (click tick icon) *

OPTIONAL TO UPLOAD ANY ATTACHMENTS, SUCH AS PHYSICAL SIGNATURE.

STEP 3: STEP 2: CLICK THE TICK ICON TO ELECTRONICALLY SIGN. ONLY THE DESIGNATED COMPLIANCE REPRESENTATIVE MAY FILL THIS OUT. THE LOGGED IN USER NAME WILL AUTOMATICALLY APPEAR. ✓

Attachments

Drop files here to upload or select.
(Maximum file size is 10 MB)