

WESTERN SYDNEY UNIVERSITY

PRACTICAL GUIDE

COMPLIANCE MANAGEMENT PROGRAM

For Designated Compliance Representatives and Nominated Compliance Contacts

UNDERSTANDING YOUR RESPONSIBILITIES, MANAGING LEGISLATIVE OBLIGATIONS AND PROVIDING COMPLIANCE ASSURANCE.

About This Guide

This guide is designed for Designated Compliance Representatives and Nominated Compliance Contacts undertaking assurance activities in Western Sydney University's Compliance Management Program.

It provides practical guidance on how to manage assigned legislation, including assessing compliance with legislative obligations, documenting key controls and supporting evidence, monitoring legislative changes, reporting non-compliance incidents, and completing annual attestations.

The guide also includes step-by-step instructions for using the University's Enterprise Governance, Risk, and Compliance (GRC) Management system and LawOne legislative alert service.

The Compliance Program Unit (CPU) provides guidance and support to assist you in fulfilling your responsibilities under the Program.

CONTACT US

Compliance Program Unit

Within the Office of University Secretary and General Counsel

General enquiries: compliance@westernsydney.edu.au

Further information:

Compliance Program website

Table of Contents

1. **UNDERSTANDING THE COMPLIANCE MANAGEMENT PROGRAM**

- Objectives — 4
- Who Does What? — 5
- Key Dates — 6
- Program Workflow — 7

2. **USING THE GRC SYSTEM**

- Logging in - 8

3. **MANAGING COMPLIANCE**

- Self-Assessments — 9
    - Reviewing Legislative Obligations — 10
    - Determining Compliance Status - 11
    - Documenting Evidence of Compliance — 12
    - What Evidence to Attach — 13
    - Understanding Compliance Controls — 14
    - How to Document Effective Controls — 15
    - Assessing Residual Risk of Non-Compliance — 16
    - Enterprise Risk Matrix for Compliance Risk - 17

4. **ANNUAL COMPLIANCE ATTESTATION**

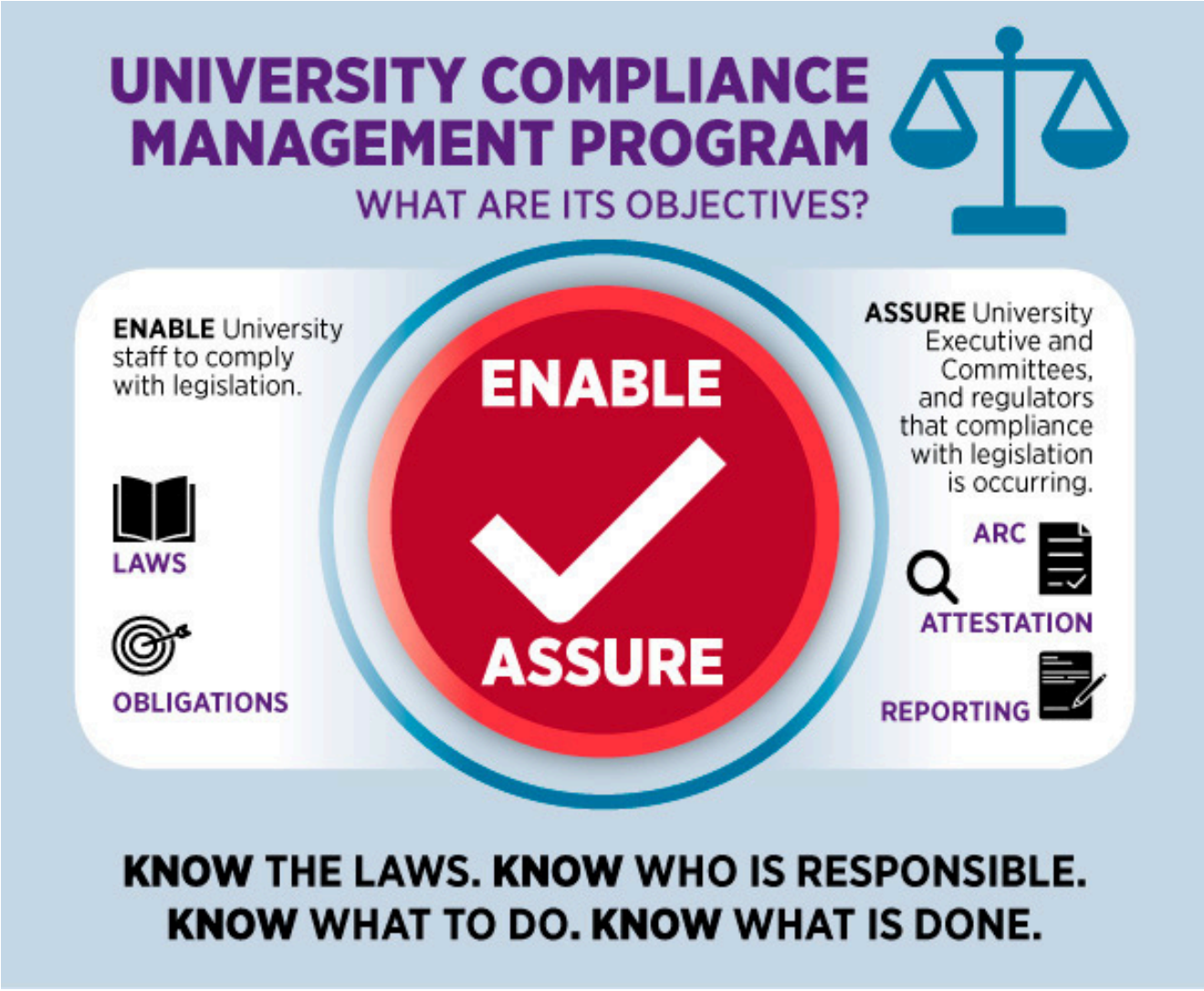
- Annual Attestations Explained — 18
- Completing your Attestation Questions — 19
- Submitting Your Annual Attestation — 20
- Compliance Representative Portfolio Attestation — 21

5. **ONGOING COMPLIANCE RESPONSIBILITIES**

- Continuous Monitoring - Reporting Incidents — 22
- Using LawOne Legislative Alerts — 23
- Quick Reference and Useful Links - 24

1. UNDERSTANDING THE COMPLIANCE PROGRAM

OBJECTIVES



EXPECTED OUTCOME:

TO *PREVENT* LEGISLATIVE NON-COMPLIANCE THROUGH EFFECTIVE *CONTROLS* AND ONGOING *MONITORING,* CONSISTENT WITH THE UNIVERSITY'S RISK APPETITE OF AVOID.

WHO DOES WHAT

Compliance is a shared responsibility across the University, operating on the **Three Lines of Defence.**

FIRST LINE – BUSINESS OPERATIONS

Owns and manages compliance.

Designated Compliance Representatives

Portfolio heads such as Executive Deans, Pro-Vice Chancellors and Chiefs.

Nominated Compliance Contacts

Subject matter experts who coordinate the day-to-day management of assigned legislation, monitor changes, report incidents and complete annual attestations.

Operational Staff and Control Owners

Carry out operational activities and implement compliance controls, processes and procedures.

SECOND LINE – OVERSIGHT AND SUPPORT

Legal, Compliance and Risk functions.

Compliance Program Unit (CPU)

Maintains the Compliance Management Program, provides guidance and support, monitors compliance risks, reviews attestations and reports compliance outcomes.

Legal and Risk

Provide specialist advice and oversight, and support the management of compliance risks and issues.

THIRD LINE – INDEPENDENT ASSURANCE

Independent review and assurance.

Internal Audit

Provides independent assurance on the effectiveness of the University's compliance arrangements, risk management and internal controls.

REPORTING AND ASSURANCE

Vice-Chancellor

Delegates to

Senior Executive Team (SET)

Delegates to

Designated Compliance Representatives

Audit and Risk Committee

↑

Senior Executive Team (SET)

↑

Compliance Program Unit (CPU)

KEY DATES

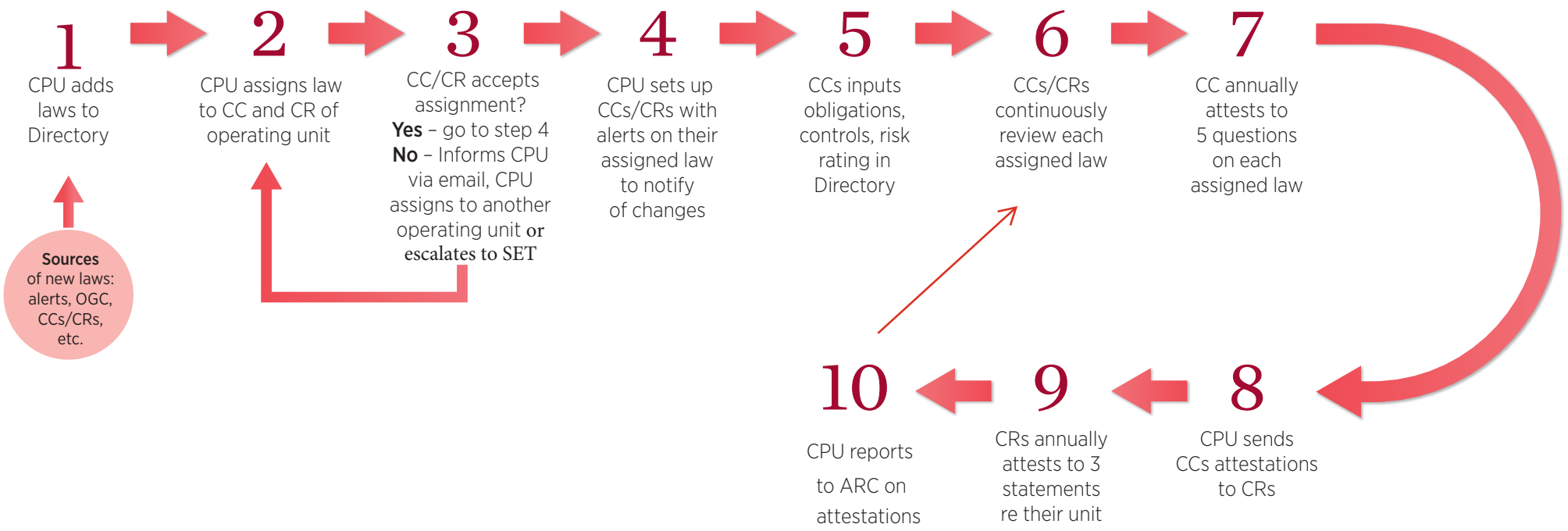
Key Dates – Annual Compliance Cycle

February and July	CPU review of legislative assignments and Compliance Directory records.
August	Confirmation of assigned legislation.
September – October	Compliance Contact annual attestations (for assigned legislation).
November – December	Compliance Representative portfolio attestations (overall compliance position for the portfolio).
Following year	Reporting of annual attestation outcomes to the Audit and Risk Committee.

Throughout the year:
Assigned legislation must be monitored, compliance assessments kept current, and potential or actual non-compliance incidents reported.

WESTERN SYDNEY
UNIVERSITY

UNIVERSITY COMPLIANCE DIRECTORY AND ANNUAL ATTESTATION PROCESS



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

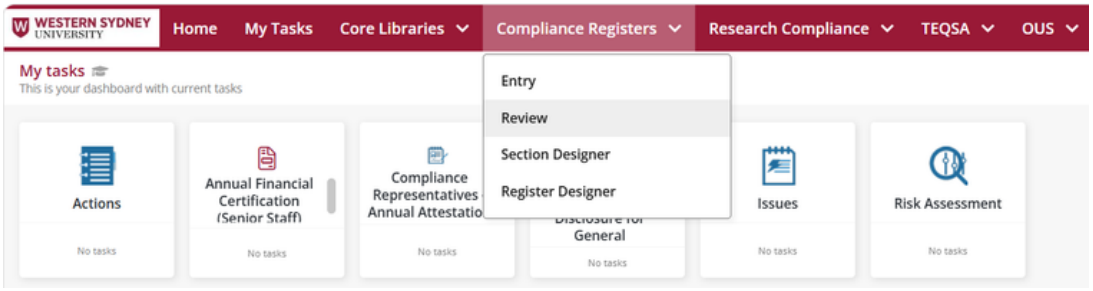
2. USING THE GRC SYSTEM

LOGGING IN

1 Go to Western.GRC system https://erm.protecht.com.au/wsu and sign in using your Western credentials (including MFA).

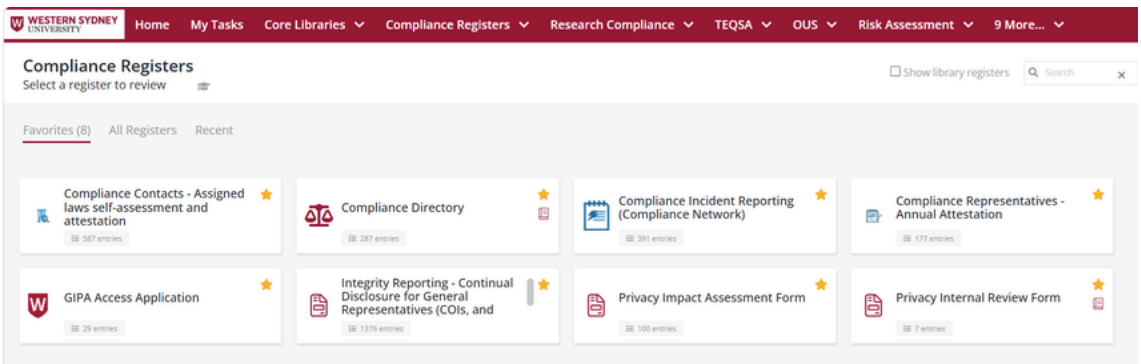
From the top menu, select Compliance Registers, then Review.

2



The Compliance Register menu to which you have access will appear.

3



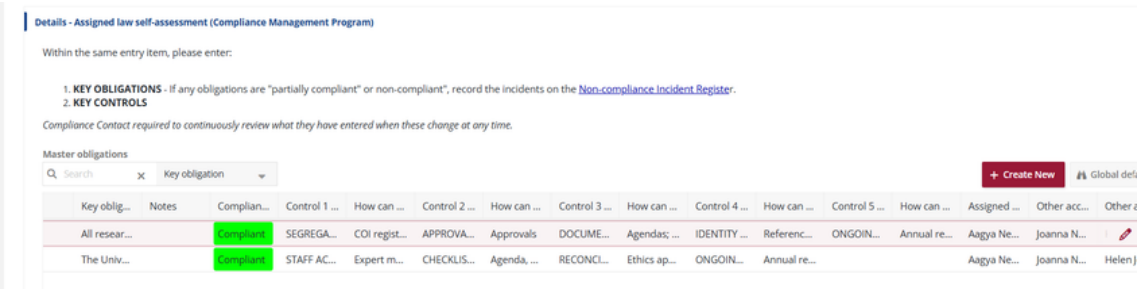
3. MANAGING COMPLIANCE

SELF-ASSESSMENTS

REQUIRED ACTION: Compliance Contacts must complete and maintain the self-assessment for each assigned law.

1. Click on "Compliance Contacts - Assigned laws self-assessment and attestation" register to view your assigned laws.

2. Scroll down to the "Assigned Law Self-Assessment" section and open each legislative obligation using the pencil icon or double-clicking.



3.



When should you update your self-assessment?

- *30 days of assignment*
- *Relevant organisational or legislative changes*
- *Whenever non-compliance incidents or control changes arise*
- *Before annual attestation.*

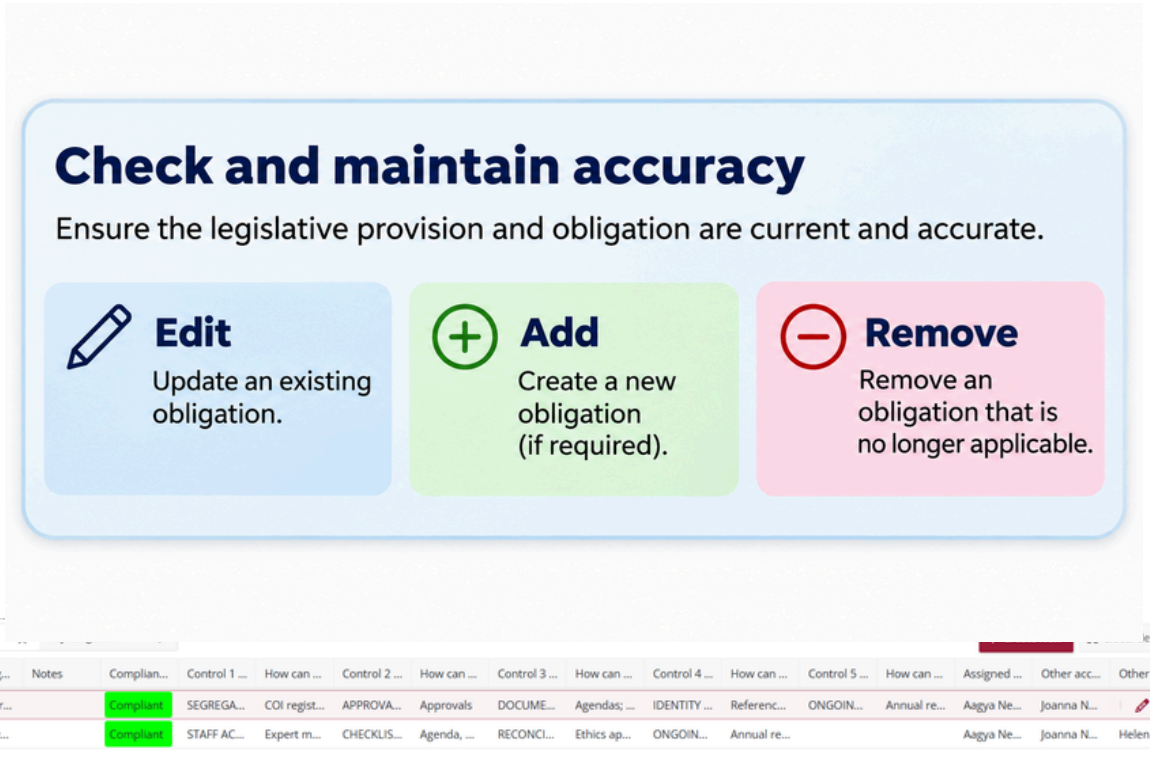
REVIEWING LEGISLATIVE OBLIGATIONS

<u>REQUIRED ACTION</u>: Compliance Contacts must review each obligation to ensure it is current, accurate, and applicable to their operating area.

Each obligation must reference the relevant legislative section or provision and identify the:

- *Positive obligation*: What the University must do.
- *Negative obligation*: What the University must not do.

Provisions that merely grant powers or permit activities (e.g. may issue a refund) are generally not obligations to be captured unless mandatory conditions apply.



DETERMINING COMPLIANCE STATUS

REQUIRED ACTION: Compliance Contacts must assess each obligation and select the appropriate compliance status.

Which status should you select?	
Compliance Status	*When to use it*
Compliant	The obligation is being met.
Partially Compliant	Some requirements are met, but compliance gaps remain. *Example: 9 of 10 required reports were submitted.*
Non-Compliant	The obligation is not being met. *Example: None of the 10 required reports were submitted.*
Unknown	Compliance has not been established and requires further assessment. *This status resets during annual attestation, requiring confirmation of the compliance position.*
N/A – Business Unit	The obligation does not apply to your operating area.
N/A – Calendar Year	The obligation applies, but the relevant activity or circumstances did not arise during the assessment year.
N/A – University Year on Year	The obligation does not apply to the University's ongoing circumstances.

Important:

- Assess compliance against the legislative requirement, not just policies, procedures or the absence of incidents.
- The selected status must reflect the actual compliance position and be supported by evidence.

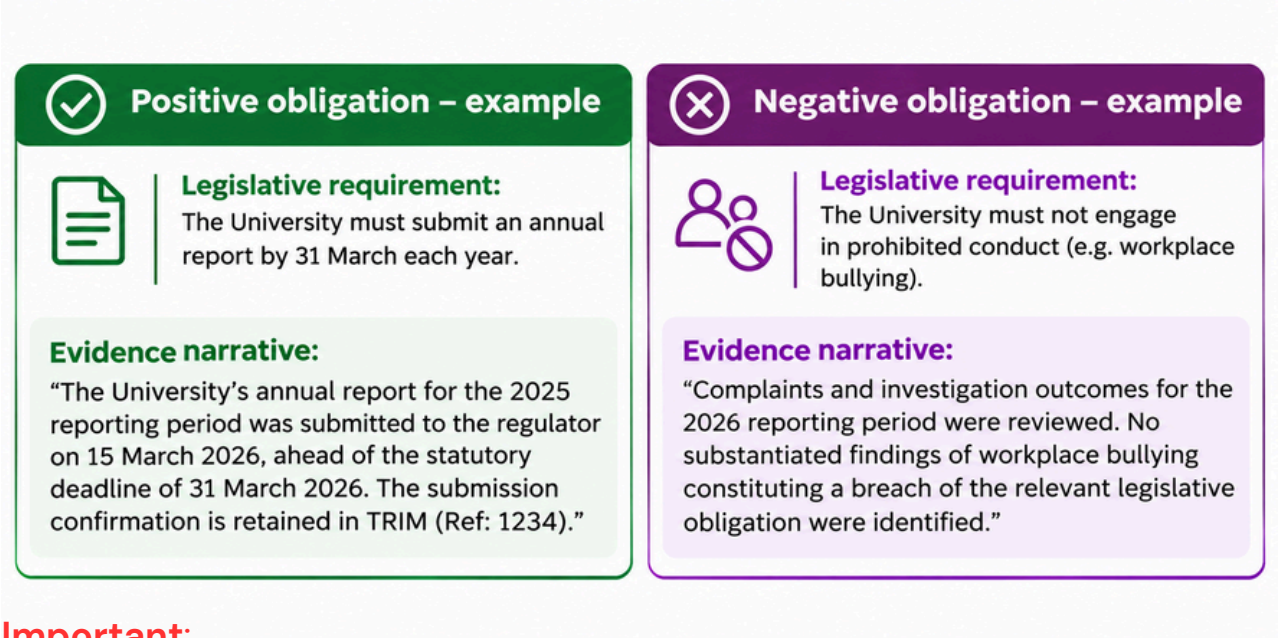
DOCUMENTING EVIDENCE OF COMPLIANCE

REQUIRED ACTION: Compliance Contacts must document how each legislative obligation is being met, using a clear and specific evidence narrative, to support the selected compliance status.

Your narrative should explain:

- *What*: What action was taken to meet the legislative obligation?
- *When*: When was the action completed, including relevant dates or reporting periods?
- *How*: How does the action demonstrate compliance with the specific legislative requirement?
- *Where*: Where is the supporting evidence maintained?

Remember: An evidence narrative must be entered to initially save the form and re-entered each time the form is updated and saved, even if the information has not changed, to maintain an audit trail.



Important:

- Evidence narratives must be verifiable and reflect the actual compliance position.
- Allegations do not automatically establish non-compliance, while the absence of incidents may support a Compliant status where appropriate controls and monitoring are in place.

WHAT EVIDENCE TO ATTACH

REQUIRED ACTION: Compliance Contacts must upload an attachment to move on with the form.

Evidence must be *relevant* to the legislative obligation.

Where supporting records cannot reasonably be uploaded, attach a brief statement explaining the circumstances and where evidence is maintained.

Reports, permits or licences	Upload the report, submission confirmation, compliance certification from the regulator, or the current permit or licence.
Event-triggered notifications	Upload the notification, or a statement confirming no event occurred that required notification.
High-volume records	Do not upload individual records. Upload a statement identifying where the records are held (e.g. HR system) and confirming they are available on request.
Prohibited conduct	Upload relevant investigation or regulatory findings, or a statement confirming no relevant adverse findings were identified following appropriate checks.

Important:
Any uploaded statement must accurately reflect the legislative obligation and the evidence available to support compliance.

UNDERSTANDING COMPLIANCE CONTROLS

REQUIRED ACTION: Compliance Contacts must identify the key controls that prevent, detect or correct non-compliance.

Compliance controls are the processes and measures used to prevent, detect or correct non-compliance with legislative obligations.



What are key controls?

Key controls are those most important to managing the risk of non-compliance with an obligation. Their failure could significantly increase compliance risk.



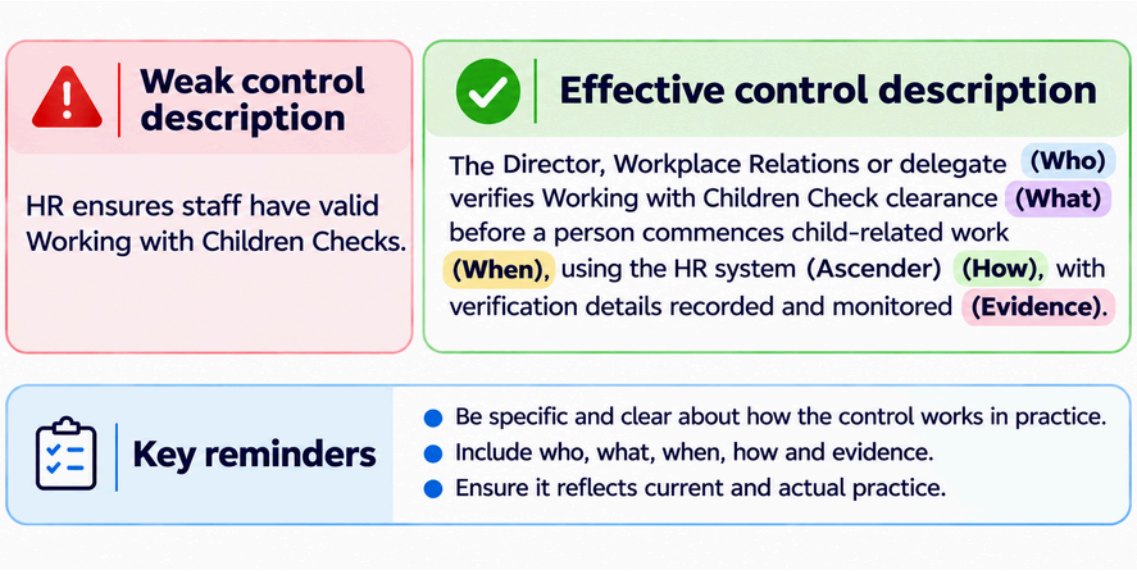
Remember:
A policy or procedure alone does not necessarily demonstrate an effective control. Explain how the requirement is implemented and monitored in practice.

DOCUMENTING EFFECTIVE CONTROLS

REQUIRED ACTION: Compliance Contacts must describe how each key control operates, including who, what, when, how and supporting evidence.



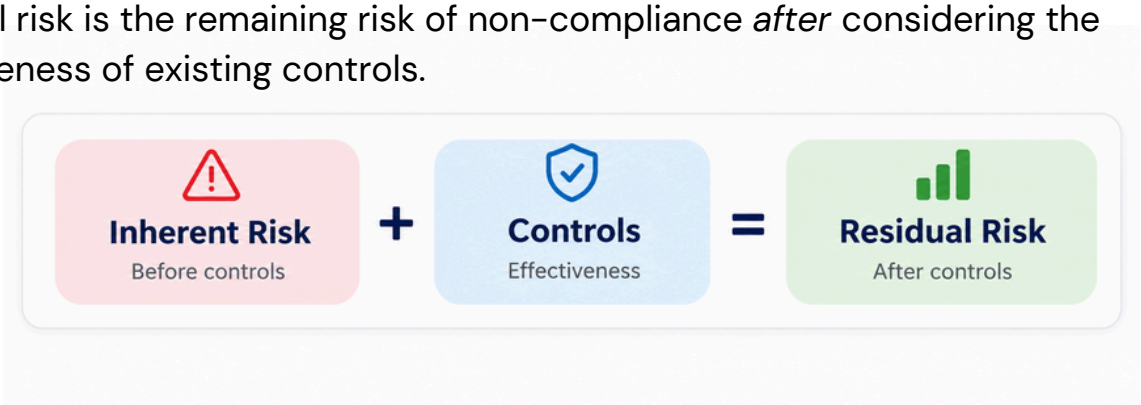
PRACTICAL EXAMPLE: Working with Children Check control



ASSESSING RESIDUAL RISK OF NON-COMPLIANCE

REQUIRED ACTION: Compliance Contacts must assess the residual risk of each assigned law, considering the effectiveness of existing controls.

Residual risk is the remaining risk of non-compliance *after* considering the effectiveness of existing controls.



Residual Risk is calculated as Likelihood x Consequence, with consideration of the control effectiveness.



Use the University's Risk Rating Matrix to determine the residual risk rating (see next page).

Remember:

- Residual risk reflects the current risk of non-compliance, considering existing controls and foreseeable changes.
- Higher ratings must be justified by likelihood, consequence, and control effectiveness, not uncertainty or concerns about external factors alone.

RISK RATING MATRIX

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

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

Likelihood

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

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

Risk Rating for Legislative Non-Compliance

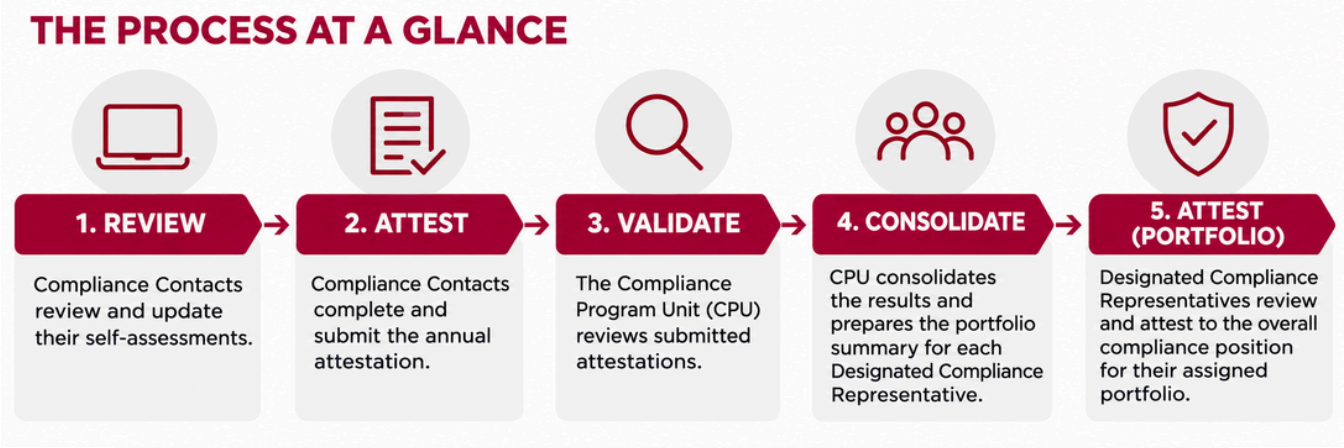
Risk Rating	
Critical	Widespread, Enterprise-wide, systemic breach of legislation, or contracts, severely affecting WSU's ability to operate including government-mandated operational changes, or loss of accreditation or license. Litigation / prosecution resulting in criminal conviction or personal liability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

4. ANNUAL COMPLIANCE ATTESTATIONS

EXPLAINED

<u>REQUIRED ACTION</u>: Compliance Contacts must i) review and update their self-assessments, then ii) complete and submit an annual attestation for each assigned law by the due date.

Annual attestation confirms the University's compliance position for the reporting year, providing assurance to the Senior Executive Team and Audit and Risk Committee.



KEY ROLES

Nominated Compliance Contacts
Review and attest to the compliance position for each assigned law.

Designated Compliance Representatives
Review and attest to the overall compliance position for their assigned portfolio, based on the consolidated information provided by CPU.

SELF-ASSESSMENT VS ATTESTATION

Self-assessment	Reflects the current compliance position and residual risk.
Annual attestation	Confirms compliance with assigned legislation for the reporting year.

REMEMBER: Ensure your self-assessment is complete, accurate and current before submitting your attestation.

COMPLETING THE ATTESTATION QUESTIONS

REQUIRED ACTION: Compliance Contacts must answer all attestation questions for each assigned law, consistent with their self-assessment.

Q1 LEGISLATIVE MONITORING

i) **Yes** — LawOne legislative alerts are supplied to Compliance Contacts as a minimum to monitor relevant amendments, with other monitoring sources (e.g. regulatory updates, sector advice) that may also be used.

ii) **No** — Legislative changes are not being adequately monitored or addressed. This increases exposure to compliance risk and should prompt a reassessment of residual risk.

Q2 CONTROLLED ENTITIES

Yes if your area performs compliance activities or controls for a controlled entity, including through shared services. Select the entities; otherwise No.

Q3 OVERALL COMPLIANCE STATUS

Select the lowest applicable status across obligations:

i) **Yes** — all applicable obligations are Compliant or N/A.

ii) **Partially Compliant** — at least one applicable obligation is Partially Compliant, and none are Non-Compliant.

iii) **Non-Compliant** — at least one applicable obligation is Non-Compliant.

Q4 EVIDENCE OF COMPLIANCE

Yes if supporting evidence for each Compliant obligation is documented or its location and custodian identified. Otherwise No; explain gaps.

Q5 INCIDENT REPORTING

i) **Yes** — incidents occurred and all were reported on the Breach Register.

ii) **No** — incidents occurred but have not all been reported.

iii) **N/A** — no incidents occurred during the calendar year.

Q6A RECORDED RESIDUAL RISK

The rating from the last self-assessment is displayed automatically. This field cannot be edited on the Attestation tab.

Q6B CONFIRM RESIDUAL RISK

Confirm whether the rating remains appropriate for the current calendar year of attesting (1 January to 31 December), considering control effectiveness, incidents, likelihood and consequence. No breaches does not automatically mean Low risk.

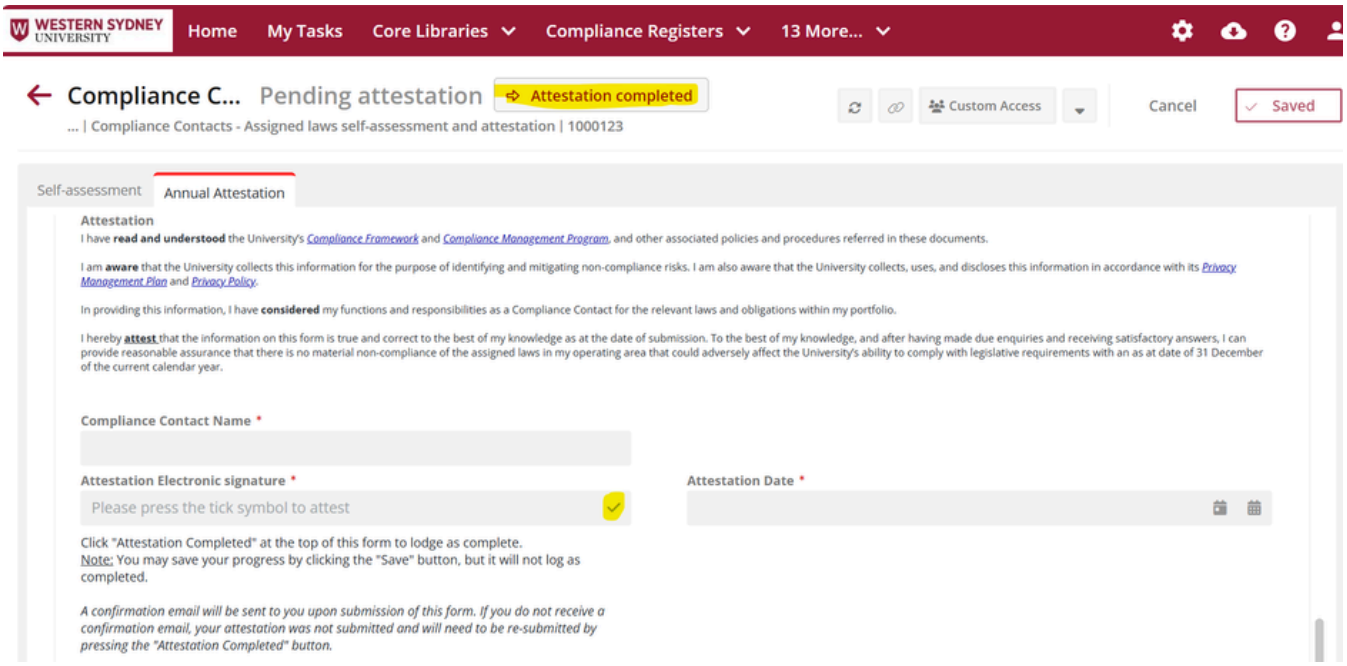
Reminder: Review your self-assessment before submitting your attestation.

SUBMITTING YOUR ANNUAL ATTESTATION

REQUIRED ACTION: Compliance Contacts must formally submit an attestation for each assigned law by the notified deadline.

How to submit

1. Review your responses and read the attestation declaration at the bottom of the tab.
2. Enter your name, electronically sign by clicking the tick icon, and enter the date.
3. Click "Attestation Completed" at the top of the page to formally submit.



Repeat for each assigned law requiring annual attestation.

Important:
Saving your responses does not constitute formal submission. You must select "Attestation Completed".

Remember:
Watchlist items do not require attestation.

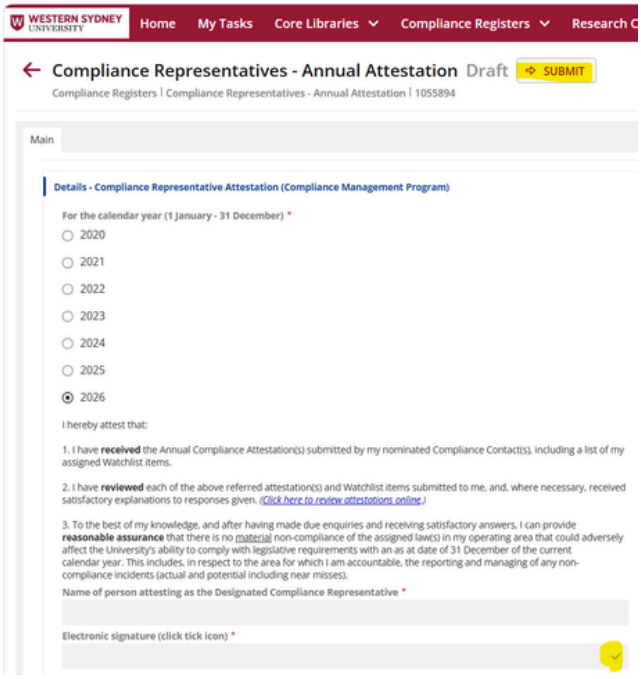
COMPLIANCE REPRESENTATIVE PORTFOLIO ATTESTATION

REQUIRED ACTION: Designated Compliance Representatives must review and attest to their portfolio's overall compliance position.

How does the process work?
Following Compliance Contact attestations, the CPU reviews submissions and provides a consolidated portfolio summary highlighting:

- *Compliance status*: Overall compliance position of assigned legislation.
- *Residual risk*: Any ratings above the University's risk appetite.
- *Non-compliance incidents*: Reported incidents and their status.
- *Concerns:* Matters affecting reasonable assurance of compliance.

Compliance Representatives must review the summary, undertake their own due enquiries and address any concerns before providing their portfolio attestation.



How to complete your attestation

1. Open the "Compliance Representatives – Annual Attestation register" in Western.GRC.
2. Complete the portfolio attestation questions.
3. Electronically sign and formally submit by the deadline.

Important:
Compliance Representatives attest separately following CPU validation; they do not approve individual Compliance Contact attestations.

5. ONGOING COMPLIANCE RESPONSIBILITIES

CONTINUOUS REVIEW – REPORTING INCIDENTS

REQUIRED ACTION: Compliance Contacts must ensure potential or actual legislative non-compliance incidents are promptly reported, managed and monitored, including incidents that have since been corrected.

How to report an incident

1. *Open* the Compliance Incident Register.
2. *Document* the circumstances, affected areas, and relevant legislation.
3. *Record* actions taken and corrective measures.
4. *Submit* the incident and update it as the matter progresses.
5. *Close* the incident by uploading evidence of remediation and completing the electronic signature.

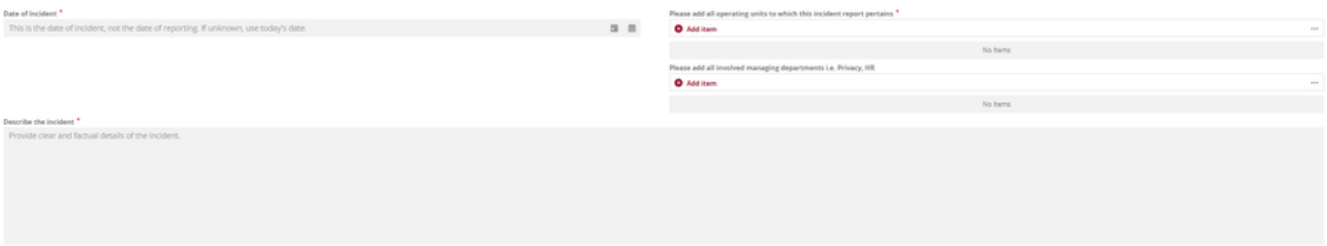
Managing reported incidents

Identify the cause of non-compliance, implement corrective actions and monitor their effectiveness to prevent recurrence.

Important:

- Report non-compliance when identified, not at annual attestation.

- Notify the Compliance Program Unit (CPU) promptly of significant compliance issues or risks.



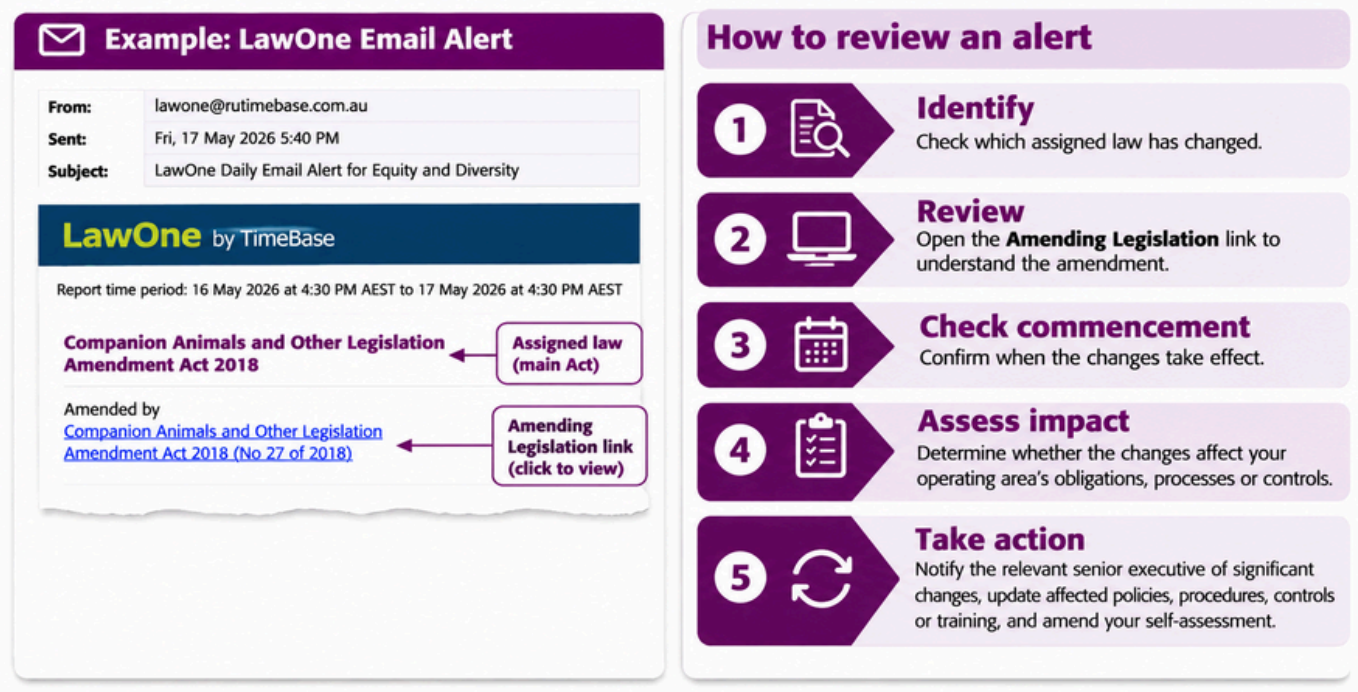
USING LAWONE LEGISLATIVE ALERTS

REQUIRED ACTION: Compliance Contacts must monitor legislative changes and take action to maintain compliance.

The CPU subscribes Contacts to LawOne alerts, sent directly to their Western email addresses.

LawOne alerts cover:

- Legislative amendments.
- New or commencing provisions.
- Repeals of legislation.
- Changes to Regulations and other subordinate legislation.



Remember:

Legislative monitoring is an ongoing responsibility, not an annual attestation activity.

QUICK REFERENCE AND USEFUL LINKS

Western.GRC — Compliance Management
Access Western.GRC
View assigned legislation, update self-assessments and complete annual attestations.

Compliance Incident Register
Report a compliance incident
Report and manage potential or actual legislative non-compliance.

LawOne Legislative Alerts
Sent direct to your Western email address.
Review legislative amendments and monitor changes affecting assigned laws.

Need assistance?
Compliance Program Unit (CPU)
compliance@westernsydney.edu.au
Contact the CPU for assistance with legislative assignments, self-assessments, attestations, incident reporting or LawOne alerts.