Risk and Compliance Policy

Purpose

This policy states the principles and requirements to manage UNSW's:

- risk management practices in its operations, activities, governance and decision-making
- legislative compliance obligations
- third-party arrangements (including commercial activities).

Scope

This policy applies to:

- UNSW and its controlled entities
- UNSW staff and affiliates
- all activities conducted by or on behalf of UNSW.

Principles and objectives

1. Risk management

Principles

1.1. UNSW is committed to promoting a culture that:

- values effective risk management as a core staff capability in making risk intelligent decisions
- encourages and supports staff to raise, discuss, treat or accept risks
- identifies, takes and manages opportunities to achieve a beneficial outcome for UNSW.

1.2. Effective risk management:

- enables strong governance and accountability
- builds a consistent risk appetite and robust risk culture
- improves decision-making, can provide competitive advantage and supports achieving UNSW's strategic objectives
- provides greater certainty and confidence to all stakeholders
- must be embedded across all areas for UNSW's continued success and growth
- should be transparent and based on the best available information
- is responsive and timely.

1.3. Adopting a structured approach in identifying, assessing and managing risk will help identify all key risks and reduce the likelihood of unexpected risks occurring.

1.4. All risks impacting UNSW's operating environment need to be considered and managed.

1.5. UNSW will consider in its decision-making the:

- scale, benefit and impact of opportunities
- associated risk exposures
- varying options available.

1.6. UNSW is committed to well-managed risk taking to achieve its strategic objectives in line with its risk appetite statements.

1.7. Risk management at UNSW broadly aligns with the key fundamentals of *ISO 31000:2018 Risk management - Guidelines*.

Objectives

1.8. Outline the risk management approach and define the risk management framework for UNSW.

1.9. Align risk management with UNSW's strategic objectives, planning and operations.

1.10. Establish and assign roles and responsibilities for risk management.

1.11. Enable UNSW's risk management to anticipate, detect, acknowledge, and respond to changes and events in a dynamic, responsive and timely manner.

1.12. Strengthen decision-making, prioritisation and planning by providing methods to assess risk and opportunity.

1.13. Continually evolve and improve UNSW's approach to risk management.

1.14. Promote a risk aware culture across UNSW.

2. Compliance management

UNSW's legislative compliance obligations require compliance management.

Principles

2.1. Compliance management is necessary and desirable.

2.2. Non-compliance may:
- create unacceptable risks for staff, students, the community and the environment
- cause physical, financial and reputational harm to UNSW
- potentially expose individuals to personal liability

2.3. Compliance must be actively promoted and supported, recognising UNSW's diversity, size and operational structures.

2.4. Effective compliance is a shared responsibility across all levels of management.

2.5. An effective system for compliance management is transparent and demonstrable.

2.6. Compliance management at UNSW broadly aligns with the key fundamentals of *ISO 37301:2021 Compliance Management Systems - Guidelines*.

Objectives

2.7. Conduct UNSW's operations in line with its compliance obligations.

2.8. Promote a culture:
- that emphasises personal accountability and ethical conduct, where behaviours that support compliance are encouraged and behaviours that compromise compliance are not tolerated
- in which compliance is an integral and natural part of UNSW's operations, without compromising efficiency or the achievement of its strategic objectives.

2.9. Assign responsibilities for compliance and ensure every level of management understands its role in managing compliance obligations.

2.10. Apply a consistent and well understood process for verifying compliance, reporting incidences of non-compliance and addressing those incidences in a timely and effective manner.

3. Third-party arrangements

Principles

3.1. Third-party arrangements will support the objectives and strategic goals of UNSW.

3.2. Commercial activities will align with the University's principal and commercial functions prescribed by the [*University of New South Wales Act* 1989 (NSW)](#).

3.3. Consistent criteria are used to evaluate third-party arrangements to meet assessments for feasibility, due diligence and integrity before they are approved.

3.4. Risk management and compliance management are applied to third-party arrangements before

approval and throughout the total life of the arrangement.

3.5. UNSW has effective governance to manage actual, potential or perceived conflicts of interest with third-party arrangements.

3.6. Third-party arrangements are appropriately managed to minimise risks of fraud, corruption or maladministration.

3.7. Third-party arrangements are stored using [UNSW Systems of Record](#).

Objectives

3.8. Define and implement processes to manage third-party arrangements.

3.9. Enable UNSW to evaluate and review the critical and high-risk third-party arrangements.

3.10. Establish and assign roles and responsibilities for third-party arrangements.

3.11. Align activities for third-party arrangements with [UNSW's risk management framework](#).
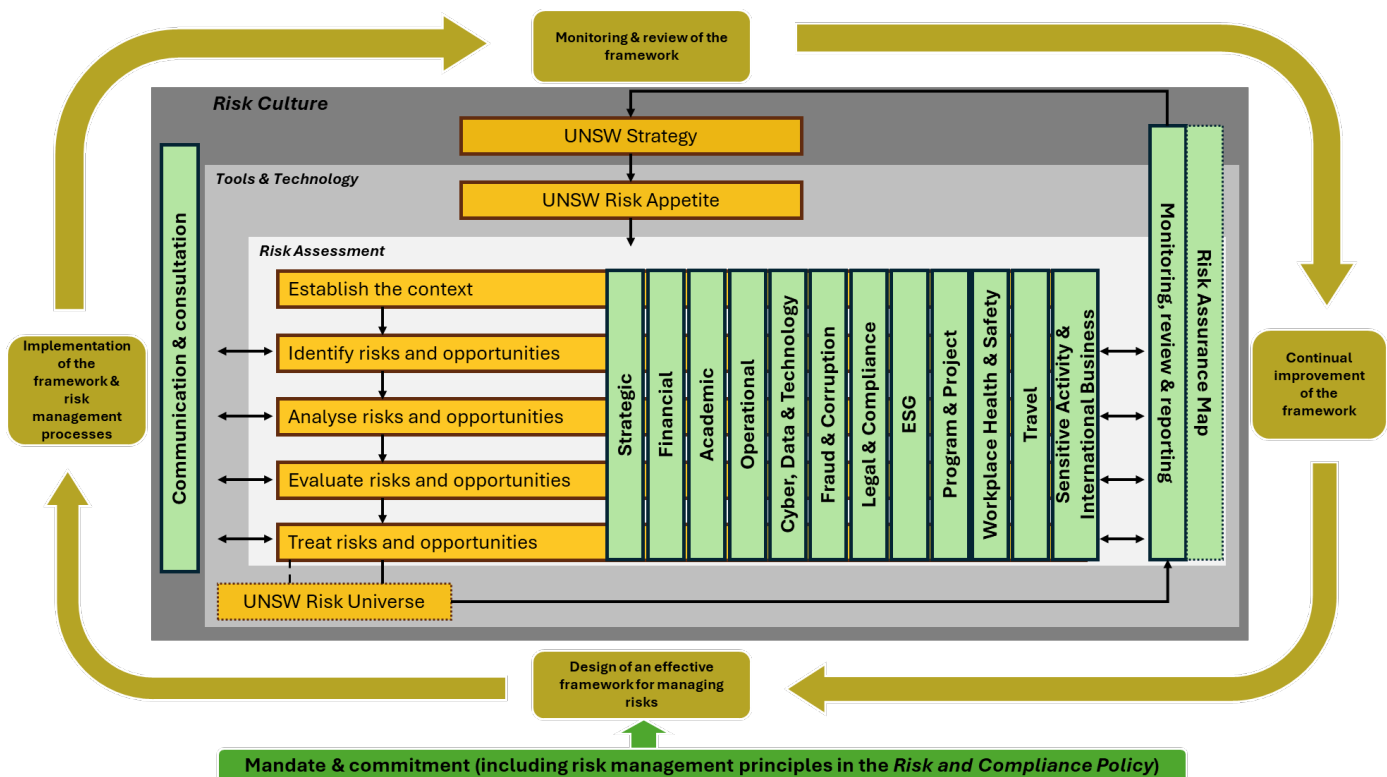
Effective: 1 June 2024   **Responsible:** DVC Transformation Planning and Assurance (DVC TPA)

Procedures – Risk management

Section 1: Risk management framework

1. Overview

1.1.　UNSW has adopted the following risk management framework:

1.2.　The risk management framework brings together UNSW's risk management principles and processes for assessing and managing risk by embedding risk management requirements into all of UNSW's activities and processes.

1.3.　All UNSW processes, activities and functions will adopt a risk management approach in line with this policy, risk management procedures and risk management framework.

1.4.　The Risk Management Manual:

- contains instructions for implementing the risk management framework
- outlines the processes to identify, assess and manage risk
- sets out where UNSW has embedded the risk management framework.

2. Risk appetite

2.1.　UNSW's risk appetite defines the level of risk that UNSW is prepared to accept to achieve its objectives. The risk appetite guides the University Leadership Team (**ULT**) in managing enterprise

strategic and operational risks and when measures are necessary to reduce the risk exposure to UNSW.

2.2. The Risk Management team, in consultation with the ULT, will annually establish the UNSW Risk Appetite statements in relation to strategic objectives. The ULT will bi-annually review these statements.

2.3. The risk appetite statements will set out the risks that UNSW:

- will not accept
- is prepared to manage
- is willing to take.

2.4. The risk appetite statements will be used to inform and review UNSW's delegations of authority.

2.5. The risk appetite statements are approved by UNSW Council.

3. Identifying, assessing and managing risks and opportunities

3.1. All areas of UNSW will follow the approach for identifying, analysing, evaluating and treating all risks and opportunities in line with section 3 *Risk & opportunity assessment* in the Risk Management Manual.

3.2. The following risk and opportunity assessments will be integrated into the normal university and local level business activities and processes:

Business activity/process	Assessment type	Frequency
Finance plan risks	Risk assessment	Every 3 – 10 years
Strategy risks		
Academic risks	Risk assessment	Annually
Environmental, social & governance risks		
Financial budgetary risks		
Fraud & corruption risks		
Legal & Compliance risks		
Operational Plan risks		
Program and project risks	Risk & opportunity assessment	Daily (ongoing)
Cyber, data & technology risks	Risk assessment	
Operations risks		
Sensitive activity and international business risks		
Travel risks		
Workplace health and safety risks		

3.3. The following process steps are used for completing risk and opportunity assessments and managing the outputs, in line with section 3 *Risk & opportunity assessment* in the Risk Management Manual:

- establish the context
- identify risks and opportunities
- analyse risks and opportunities
- evaluate risks and opportunities
- treat risks and opportunities
- communication and consultation

- monitor, review & reporting.

4. Risk universe and assurance map

4.1.   The UNSW Risk Universe:

- sets out the risks that UNSW faces or could face across its operations
- is a formal part of UNSW's risk identification process
- is not static and is regularly reviewed and updated by the Risk Management team.

4.2.   The UNSW Risk Assurance Map:

- is a visual representation of the main sources and types of assurance activities at UNSW
- demonstrates the scope, breadth and depth of assurance coverage and their coordination across the UNSW Risk Universe.

4.3.   The Risk Management team will use risk, management and assurance reviews, risk assessments and Internal Audit activity to develop and maintain the UNSW Risk Universe.

4.4.   The Risk Management team will update the UNSW Risk Universe annually at minimum by considering the risk assessments that have been done and UNSW's risk management framework, including the "three lines model" (refer to section 4 *Ongoing risk management* in the [Risk Management Manual](#)). These outputs will be considered in UNSW's Risk Assurance Map.

5. Monitoring, reviewing and improving the risk management framework

5.1.   The Risk Management team, in consultation with the ULT, will annually review the risk management framework to identify:

- required operational changes
- regulatory or standard changes
- other improvements.

5.2.   The Director of Risk will inform the Safety and Risk Committee of Council of any updates or changes to the risk management framework.

6. Reporting

6.1.   All staff must report risks in line with this policy, risk management procedures and risk management framework.

Section 2: Roles and responsibilities

1. UNSW Council

1.1.   UNSW Council must fulfil its obligations to risk management in line with the *[University of New South Wales Act 1989 (NSW)](#)*.

2. Safety and Risk Committee of Council

2.1.   The Safety and Risk Committee of Council must fulfil its obligations to risk management in line with their [Terms of Reference](#).

3. Vice-Chancellor

3.1.   The Vice-Chancellor:

- assigns responsibilities for risk management

- provides timely and adequate information to Council on the status of UNSW's key risks
- proposes, in consultation with the ULT, UNSW's tolerance in accepting certain risks e.g. risk appetite statements
- is responsible for the risk management culture across UNSW.

4. Senior leaders and managers

4.1. Senior leaders (e.g. Provost, Deputy Vice-Chancellors, Vice-Presidents, Deans, Chief Officers and Directors) and managers responsible for leading business processes or risk controls (e.g. Heads of School/department/unit):

- design, develop, operate and maintain business processes and risk controls to manage and reduce risks while aligning with UNSW's risk appetite
- responsible for understanding this policy, risk management procedures and risk management framework, and building awareness of them across their areas of responsibility
- create and maintain a risk aware culture, including committing to and demonstrating risk awareness in decision-making
- report and escalate risk
- provide feedback on this policy to the Director of Risk
- ensure management reviews are done annually on business processes and their risk controls to ensure they are meeting their purpose for managing risk e.g. reducing key risks
- report the outcomes of the management reviews, including any critical or high risks identified, to their manager
- report annually the results of all management reviews to the [Risk Management team](#) and [Legal & Compliance](#).

4.2. Performance and a commitment to risk management will form part of the annual performance and review process for senior leaders and managers.

5. Staff

5.1. Staff that manage, monitor and review operational activities (e.g. Payroll Manager, HR Manager, Safety Manager etc.):

- provide advice and support for managing risk
- develop, implement and continuously improve risk management practices (including risk controls) within their areas of responsibility
- achieve risk management objectives such as compliance with laws and regulations, acceptable ethical behaviour, quality assurance, risk controls, sustainability etc.
- implement processes, frameworks, and guidelines for staff to manage risk
- provide analysis and reports on the adequacy and effectiveness of risk management (including risk controls) in continuously improving and achieving risk management objectives
- provide training and tools to embed risk management across operational activities, improve staff risk management capabilities and support risk awareness in decision-making
- report and escalate issues and emerging risks to senior leaders
- support and provide input into reviews for senior leaders.

5.2. Staff that perform operational activities (e.g. Professors, Associate Professors, Chief Investigators, Accounts Payable Officers etc.):

- responsible for understanding UNSW's risk management framework
- identify, assess and manage risks in their activities
- report and escalate to their supervisor any critical, high or increasing medium risks that have not been addressed
- follow defined processes, activities and risk controls
- adhere to delegations of authority and risk appetite limits

- provide feedback on existing business processes and risk controls to their supervisor.

6. Risk Management team

6.1.   The [Risk Management team](#):

- implements this policy and risk management procedures
- implements and embeds the risk management framework across UNSW
- reports key risks and risk management framework matters, to the ULT, senior management and the Safety and Risk Committee of Council
- advises ULT and the senior management on emerging or significant risk exposures
- advises ULT and the senior management on the risk management culture across UNSW
- provides and oversees the allocation of resources to enable effective risk management at UNSW
- supports communication and consultation activities by preparing reports and providing advice and guidance on risk management matters
- facilitates discussions and solutions on areas of risk uncertainty across UNSW
- provides training across UNSW on applying the risk management framework.

7. Internal Audit

7.1.   Internal Audit:

- is responsible for independent reviews and reporting on the design and operational effectiveness of internal controls, such as risk controls and compliance controls
- maintains and reports on UNSW's Risk Assurance Map, in consultation with the Risk Management team, highlighting to relevant stakeholders any significant gaps in coverage or areas that have had multiple reviews within a short period of time.

Effective: 1 June 2024   **Responsible:** DVC TPA   **Lead:** Director of Risk

Procedures – Compliance management

Further details on the compliance management procedures are available in the [Compliance Management Instructions](#).

Section 1: Documenting and classifying compliance obligations

1. Documenting compliance obligations

1.1.   Identified compliance obligations must be documented in the online Compliance Obligations Register (the **Register**) by the University Compliance Owner (**UCO**), in collaboration with the Compliance & Privacy Law team.

1.2.   An identified compliance obligation (the **core obligation**) will be separated into sub obligations where necessary to effectively manage the obligation.

1.3.   The Register must include the following information for each core obligation and sub obligation:

- overview
- legislative source
- consequences of non-compliance
- classification tier (refer to sub-section 2.2 below)
- applicable business units
- management framework (refer to sub-section 1 of the [Managing compliance obligations](#) procedure)
- internal compliance controls implemented (refer to sub-section 2 of the [Managing compliance obligations](#) procedure)
- Control Effectiveness Rating (refer to sub-section 1.5 of the [Compliance assurance and certification](#) procedure)
- certification results (refer to sub-section 2 of the [Compliance assurance and certification](#) procedure)
- any compliance issues (refer to sub-section 2.4 of the [Reporting and managing a compliance issue](#) procedure)

2. Classifying compliance obligations

2.1.   Compliance obligations are classified using a risk based approach that reflects the consequences of non-compliance with the obligation. This also determines the requirements of certification for the compliance obligation. Refer to the risk consequence table in *Appendix 1: Risk & opportunity assessment criteria* in the [Risk Management Manual](#) for further guidance.

2.2.   A four-tiered system is used for classifying compliance obligations:

RISK CONSEQUENCE – SEVERE OR MAJOR			
Tier	**Description**	**Central management**	**Certification**
1	University-wide compliance obligations where a breach could result in personal liability of individuals or have a **severe or major** consequence on the operation of the entire University or school(s) / department(s)/division(s).	Yes, compliance must be centrally managed. e.g. *Tertiary Education Quality and Standards Agency Act 2011* (Cth) – meet the Higher Education Standards Framework (Threshold Standards)	Annually
2	Compliance obligations relevant to a single school/department, or a limited number of schools/departments, where a breach could result in personal liability of individuals or have a **severe or major** consequence on the operation of the school(s) or department(s).	Yes, compliance must be centrally managed. e.g. *Radiation Control Act 1990* (NSW) - maintain effective radiation management procedures and obtain all necessary licences	Annually
RISK CONSEQUENCE – MODERATE, MINOR OR INSIGNIFICANT			
Tier	**Description**	**Central management**	**Certification**
3	University-wide compliance obligations where a breach could have a **moderate, minor or insignificant** consequence on the operation of the entire University.	Yes, compliance must be centrally managed. e.g. *Fringe Benefits Tax Assessment Act 1986* (Cth) – meet all obligations under the fringe benefits tax rules	Every 2 years
4	Compliance obligations relevant to a single school/department, or a limited number of schools/departments, where a breach could have a **moderate, minor or insignificant** consequence on the operation of the school(s) or department(s).	No, compliance can be locally managed. e.g. *Building Energy Efficiency Disclosure Act 2010* (Cth) – disclose energy efficiency of a building when selling or leasing all or part of the building	As required

2.3.   The tier of the compliance obligation will be documented in the Register by the Compliance & Privacy Law team, in collaboration with the UCO.

Section 2: Managing compliance obligations

1. Management framework

1.1.   Each core obligation and sub obligation must have a management framework comprising:

- *Executive Responsibility* – the University Leadership Team (**ULT**) member that has oversight in managing the obligation
- *University Compliance Owner* – the University officer responsible for identifying, developing, implementing and monitoring internal compliance controls for managing the obligation. The UCO is also responsible for monitoring any changes to the obligation and updating internal compliance controls to ensure the obligation is managed effectively.

- *Operational Responsibility* – the University officers responsible for ensuring internal compliance controls are applied in their business unit for managing the obligation.

1.2.   The Vice-Chancellor, in consultation with the ULT as required, will determine the management framework for a compliance obligation where it cannot be determined based on portfolio responsibilities.

1.3.   The Compliance & Privacy Law team, in consultation with UCOs, will update the management framework for compliance obligations as soon as possible when there is a change to portfolio responsibilities.

1.4.   The management framework of the compliance obligation must be documented in the Register by the UCO, in collaboration with the Compliance & Privacy Law team.

2. Internal compliance controls

2.1.   Compliance obligations are managed by the UCO through internal compliance controls (**compliance controls**). Compliance controls are systems and processes that reduce the risk of non-compliance with legislative obligations.

2.2.   Each compliance obligation must have compliance controls that:

- prevent the likelihood of a breach occurring
- detect a breach occurring
- correct the breach by reducing its impact and preventing reoccurrence.

2.3.   When developing compliance controls, the UCO will:

- assess all compliance obligation risks to UNSW in line with sub-sections *Analyse risks & opportunities* and *Evaluate risks & opportunities* in the [Risk Management Manual](#)
- apply a risk management approach and develop compliance controls which are appropriate to the assessed levels of risk and reflect the tiered-classification rating for the obligation
- document evidence for reporting and remediation e.g., operating procedures or delegations that justify the exercise of power through auditable records
- balance the operational needs of UNSW to perform its functions efficiently while remaining compliant by considering the measures (such as training, monitoring and checks) that may be required to implement the compliance controls.

2.4.   Compliance controls must adequately address the risks of non-compliance while being practical and cost-effective. Compliance controls should also adapt to reflect changes in UNSW's operating environment.

2.5.   The compliance controls for a compliance obligation must be documented in the Register by the UCO, in collaboration with the Compliance & Privacy Law team.

Section 3: Licences and permits

1. Obtaining and complying with licences and permits

1.1.   UNSW must obtain licences and permits where required to lawfully conduct an activity.

1.2.   Compliance controls must be implemented to ensure compliance with the licence or permit. Such controls must be monitored, which may include periodic inspections or audits.

2. Holder of a licence or permit

2.1.   Licences and permits must be held in the name of UNSW unless it is required by law or regulatory

practice to be held in the name of an individual.

2.2.   Where a licence or permit is held in the name of an individual:

- the individual must have primary responsibility for the activity relating to the licence or permit
- the UCO responsible for the licence or permit must approve the individual
- UNSW must employ the individual
- there must be internal controls for the cancellation, re-issue or transfer of the licence or permit if the individual no longer has primary responsibility for the activity or if they are no longer employed by UNSW.

3. Applying for a licence or permit

3.1.   The UCO must establish an approval process to apply for a licence or permit from an issuing authority.

3.2.   The approval process must include an assessment for requiring the licence or permit and UNSW's ability to comply with all terms and conditions. Records of the approval, assessment and application must be kept for all licences and permits in a UNSW System of Record.

4. Documenting licences and permits

4.1.   All UNSW licences and permits must be documented in the Register with details such as:

- name of the licence or permit (including legislation under which it is issued)
- issuing authority (Government department, agency or other regulatory body)
- holder of the licence or permit
- expiry date of the licence or permit
- individual that approved the application
- activity for which the licence or permit has been obtained
- any specific terms and conditions
- any breaches of the licence or permit notified by or to the issuing authority.

Section 4: Compliance assurance and certification

1. Assurance of compliance controls

1.1.   Each compliance control must be assessed at least annually to determine how effective it is at preventing the likelihood or reducing the impact of a compliance breach.

1.2.   Where a compliance control applies to several compliance obligations, it should be assessed against each obligation.

1.3.   The compliance control must be assessed using the following characteristics for internal controls:

Characteristic	Description
Relevance	*Does the internal control support effective compliance with the obligation?* The compliance control may be relevant to some obligations but not others.
Coverage	*Does the internal control address compliance for part of an obligation, all of the obligation or multiple obligations?* It needs to be identified when the compliance control only addresses part of a compliance obligation.

Reliability	*Does the internal control work all the time?* It needs to be determined if the compliance control is automated or a manual process. It also needs to be determined if the compliance control works under all scenarios and conditions.
Reactivity	*Is the internal control quick enough to prevent the likelihood or reduce the impact of a compliance breach?* The compliance control must operate at an appropriate speed when it addresses an event or circumstance.
Availability	*Are there sufficient resources for the internal control to operate as intended?* Some compliance controls are complex and to perform correctly require expertise. Some compliance controls to be effective require specific types of staff.
Monitored	*Is the internal control monitored or reviewed?* A compliance control is only effective when it is implemented and reviewed to ensure it is working as intended.

1.4.   Additional characteristics may be used to assess a compliance control depending on the compliance obligation that it is being assessed against.

1.5.   Each compliance control is given a Control Effectiveness Rating based on its assessment against the characteristics in sub-sections 1.3 and 1.4:

Control Effectiveness Rating	Description
Effective	The compliance control is adequate, appropriate and effective. It supports effective compliance with the obligations.
Well-based	A few weaknesses in the compliance control have been identified. However, it still supports effective compliance with the obligations.
Improvement desired	Numerous weaknesses in the compliance control have been identified. It is unlikely to support effective compliance with the obligations.
Ineffective	The compliance control is not adequate, appropriate or effective. It does not support effective compliance with the obligations.

1.6.   The Control Effectiveness Rating must be documented in the Register by the UCO, in collaboration with the Compliance & Privacy Law team.

2. Compliance certification of obligations

2.1.   All compliance obligations must be certified regularly by the UCO to record how they are being managed by UNSW. Core obligations and sub obligations must be certified as least:

- Tier 1 – Annually
- Tier 2 – Annually
- Tier 3 – Every 2 years
- Tier 4 – As required.

2.2.   Where a core obligation is not separated into sub obligations, it will be certified the same way as a sub obligation (refer to sub-section 2.4).

2.3.   Where a core obligation is separated into sub obligations, the certification of the core obligation will

make an assessment based on the results from certifying each sub obligation.

2.4. The certification of a sub obligation will:

- confirm that the management framework is up to date
- confirm that any changes to the obligation (e.g. through legislative amendments) have been identified and addressed
- assess the latest Control Effectiveness Rating for each compliance control
- confirm that all actual or potential compliance breaches have been reported in line with the Reporting and managing a compliance issue procedure and that agreed actions have been, or are in the process of being, implemented.

2.5. The results of each completed certification must be documented in the Register by the Compliance & Privacy Law team.

Section 5: Reporting and managing a compliance issue

1. Reporting a compliance issue

1.1. A compliance issue is an incident, event or situation where there is an actual, suspected or potential breach of a compliance obligation. A compliance issue is reported so actions can be implemented to prevent reoccurrence.

1.2. Unless the compliance issue relates to *serious wrongdoing* (see sub-section 1.3 below):

- the staff member must report the compliance issue to their supervisor as soon as possible after becoming aware of the issue
- the supervisor must then report the compliance issue to their Head of School or department
- if there is no one appropriate within the school or department to report the compliance issue, then it should be reported to the compliance obligation's UCO or to Legal & Compliance
- the staff member should report the compliance issue whether it involves themself or someone else.

1.3. If the compliance issue is due to an honest and reasonable belief of *serious wrongdoing*, the staff member should make a Public Interest Disclosure in line with sub-section 7.1 in the Public Interest Disclosure (Whistleblowing) Policy and Procedure. The purpose of this notification is to enable the Conduct & Integrity Office to assess the disclosure and provide advice to the Vice-Chancellor & President if they must notify ICAC as required by the *Independent Commission Against Corruption Act 1988* (NSW).

2. Managing a compliance issue

2.1. Where a compliance issue is reported to the Head of School or department, they must immediately:

- conduct a preliminary investigation in line with UNSW policies and procedures and implement actions to prevent or contain the compliance breach
- notify the compliance obligation's UCO that a compliance issue has been reported and the actions that have been taken to prevent or contain the compliance breach.

2.2. The UCO (or their nominee) will assess the severity of the compliance issue and provide instructions to the Head of School or department on the actions required to prevent reoccurrence. The school or department is responsible for implementing the actions unless the UCO determines it is necessary to intervene.

2.3. Where there is a duty to report the compliance issue to an external regulatory body, the UCO will make the report on behalf of UNSW in line with any statutory requirements.

2.4. The UCO must notify [Legal & Compliance](#) where there is a duty to report the compliance issue to an external regulatory body or the compliance issue is likely to create other legal risks (e.g. claims against UNSW). Details of the compliance issue, advice given and actions implemented must be documented in the Register.

2.5. A compliance issue will be closed in the Register once the UCO is satisfied that all necessary actions and additional compliance controls have been implemented. If a broader risk to UNSW is identified, then the compliance breach is reported to the Director of Risk for inclusion in the University Risk Register.

2.6. Documenting compliance issues in the Register provides the basis for reporting to UCOs, senior leaders, ULT and the committees of the University Council.

2.7. Compliance issues in the Register are confidential and may include legal advice with legal professional privilege attached. Staff should not disclose the information to anyone outside of UNSW without prior approval of [Legal & Compliance](#).

Section 6: Reporting to University Leadership Team and Council

1. Annual reporting

1.1. Legal & Compliance provides an annual report on compliance management to the ULT and the Safety and Risk Committee of Council.

1.2. The annual report includes:

- compliance assurance and certification results
- compliance issues
- emerging compliance obligations.

2. Additional reporting

2.1. Additional reports on compliance issues may be provided to the ULT or Safety and Risk Committee of Council as required.

Section 7: Roles and responsibilities

1. University Leadership Team (ULT)

1.1. The ULT:

- assist the Vice-Chancellor to determine compliance responsibilities as required (e.g. where no UCO has been determined for a compliance obligation)
- provide resources to manage compliance obligations
- review and make recommendations for the annual report
- endorse the annual report to be tabled at the Safety and Risk Committee of Council.

1.2. Individual ULT members:

- provide resources to manage compliance obligations
- oversee the management of compliance obligations
- oversee UCO responsibilities of their compliance obligations (refer to sub-section 1.1 of the [Managing compliance obligations](#) procedure).

2. University Compliance Owners (UCOs)

2.1. UCOs:

- document and classify their compliance obligations in the Register (in collaboration with Legal & Compliance)
- monitor any changes to their compliance obligations (e.g. as a result of a change in law) and update internal compliance controls to ensure the obligation is managed effectively
- develop and implement compliance controls for compliance with obligations and licences or permits
- liaise with senior leaders and other key internal stakeholders to ensure that compliance controls are being correctly applied in all areas of UNSW having the compliance obligations
- work with senior leaders to resolve reported compliance issues and ensuring relevant compliance issues are reported to [Legal & Compliance](#)
- assess compliance controls and completing compliance certifications in line with the schedule provided by [Legal & Compliance](#)
- provide reports as required.

3. Senior leaders

3.1. Senior leaders (e.g. Heads of School/department/unit, Chief Officers and Directors):

- understand this policy, compliance management procedures and instructions, and build awareness of them across their areas of responsibility
- ensure all relevant compliance controls for compliance with obligations and licences or permits are applied within their school or department
- ensure compliance with terms and conditions of licences or permits within their school or department
- report all compliance issues that occur in their school or department
- take action for resolving compliance issues and as directed by the UCO
- provide feedback on this policy to the Head of Compliance & Privacy Law.

4. Compliance & Privacy Law team

4.1. The Compliance & Privacy Law team within Legal & Compliance:

- implements the compliance management procedures in this policy
- maintains the management framework for compliance obligations, in consultation with UCOs
- provides advice on compliance obligations and compliance issues
- coordinates the documenting and classifying of compliance obligations in the Register
- maintains the Register
- schedules and conducts the assurance of compliance controls and compliance certification of obligations
- prepares reports to the ULT and Safety and Risk Committee of Council as required.

5. Staff

5.1. All other staff:

- are responsible for being aware of their compliance management responsibilities and following compliance controls as directed by their supervisor
- must report actual, suspected or potential compliance issues in line with sub-section 1 of the [Reporting and managing a compliance issue](#) procedure.

Procedures – Third-party arrangements

Section 1: Defining a third-party arrangement

1. What is a third-party arrangement?

A third-party arrangement exists when sub-sections 1.2 and 1.3 apply.

1.1.   A third-party arrangement is an arrangement in any form of writing between:

- UNSW, faculties, schools, divisions, business units or centres; and
- a person, company or organisation which is external to UNSW, located in Australia or overseas.

1.2.   A third-party arrangement is any activity engaged by or on behalf of UNSW in performing commercial functions, such as:

- commercialising intellectual property
- providing services to an external party for a fee (e.g. consulting, contract research)
- leasing, licensing and hiring of space/facilities to an external party
- short course offerings (e.g. non-award courses for professional development, workshops or other events charging a fee for the delivery of continuing professional education/accreditation)
- selling non-academic goods (e.g. merchandise)
- establishing or participating in a partnership, trust or controlled entity (local or overseas) to perform an activity that is mainly commercial
- establishing or operating a joint venture (in which UNSW is not acquiring a controlling interest) to perform an activity that is mainly commercial.

1.3.   Third-party arrangements can be described as a collaboration, alliance or partnership. They may or may not be legally binding and will not always have financial benefits to UNSW.

2. What is not a third-party arrangement?

2.1.   Arrangements outlined in sub-sections 2.2 – 2.5 are not third-party arrangements for the purpose of this policy.

2.2.   Arrangements between UNSW and its employees, conjoint staff or other honorary positions. These arrangements are managed by UNSW's human resources and recruitment processes.

2.3.   Arrangements between UNSW and its students for providing education, accommodation and other services. These arrangements are managed by UNSW's processes for admission and enrolment, accommodation and student services.

2.4.   Business as usual research arrangements that are managed by UNSW's research funding processes. This includes agreements for funding research or conducting clinical trials between UNSW and:

- Commonwealth, State and other Australian government or funding agencies (e.g. NHMRC, ARC, Medical Research Future Fund, Cancer Institute NSW)
- local health districts or private hospitals

- Australian industry partners (e.g. in connection with funding schemes and agencies such as ITRP, CRCP and Arena).

2.5.   Examples of business-as-usual research arrangements include:

- research collaboration agreements between UNSW (as the lead or as a collaborator) and other Australian universities or research institutes
- funding that has been provided by one of the funding agencies or industry partners in sub-section 2.4
- clinical trial research agreements with Australian health services
- UNSW entering a research contract with an Australian-based third-party in its own name, on behalf of an affiliated medical research institute.

Section 2: Critical and high-risk third-party arrangements

1. Determining critical and high-risk third-party arrangements

1.1.   A third-party arrangement is critical or high-risk when any of sub-sections 1.3 – 1.22 apply.

1.2.   A critical or high-risk arrangement must have additional controls in line with sub-section 3 [Controls for critical & high-risk third-party arrangements](#) in this procedure.

A third-party arrangement is critical or high-risk if the arrangement has activities or requirements that:

1.3.   Fall outside of [UNSW's risk appetite](#) (refer to sub-section 2 of the [Risk management framework](#) procedure).

1.4.   Involve critical technology, infrastructure or materials on the [Defence & Strategic Goods List (DSGL).](#)

1.5.   Involve a party in a country that is currently subject to sanctions imposed by the Australian Government

1.6.   Involve a party in a country with a [Transparency International Corruptions Perception Index](#) (CPI) below 50.

1.7.   Require additional disclosures or activities to comply with the requirements under the foreign interference guidelines and national security legislation.

1.8.   Potentially place the [health and wellbeing](#) of UNSW staff or students at risk.

1.9.   Enable serious abuse of human rights, animal rights or the environment.

1.10.   Involve technology that can potentially counter [UNSW's core values](#).

1.11.   Involve a third-party using UNSW's trademarks, brands or logos in a prominent way (other than purely for educational purposes) without obtaining prior consent from UNSW in writing.

1.12.   Involve UNSW endorsing or sponsoring a third-party or its goods or services.

1.13.   Involve conditions that counter UNSW practices, policies and procedures.

1.14.   Limit UNSW's freedom of enquiry or academic freedom.

1.15.   Restrict future UNSW activities (e.g. non-compete clause).

1.16.   Involve UNSW receiving significant funding from a:

- private donor; or
- bequest, will or gift from a third-party; or

- a foreign government

that involves:

- naming rights to a university building or institute; or
- establishing named chairs or other positions at UNSW.

1.17.   Involve entering into an agreement with a third-party (not including Australian Government or Universities) where it assumes UNSW:

- has uncapped liability
- would incur liquidated damages
- has no exclusion of consequential loss, or
- gives indemnities for the negligence of other parties

if the agreement is not delivered within set milestones.

1.18.   Involve entering into an agreement with a third-party where UNSW's aggregate liability is above 4 times the total fees received by UNSW.

1.19.   Involve entering into an agreement with a third-party where UNSW provides indemnities or warranties for acts, activities or matters beyond its control.

1.20.   Involve a third-party developing, purchasing, leasing (except for retail purposes) or occupying UNSW's land or buildings, including:

- contracts with third parties relating to major capital works to UNSW campus
- co-location of industry at UNSW.

1.21.   Involve UNSW making a significant investment in a third-party, which may include an agreement to accept equity in that third-party or extending substantial financial support to that third-party through a loan.

1.22.   Expose UNSW to a risk that is rated as critical or high (refer to sub-section 3 of the [Risk management framework](#) procedure for assessing risks).
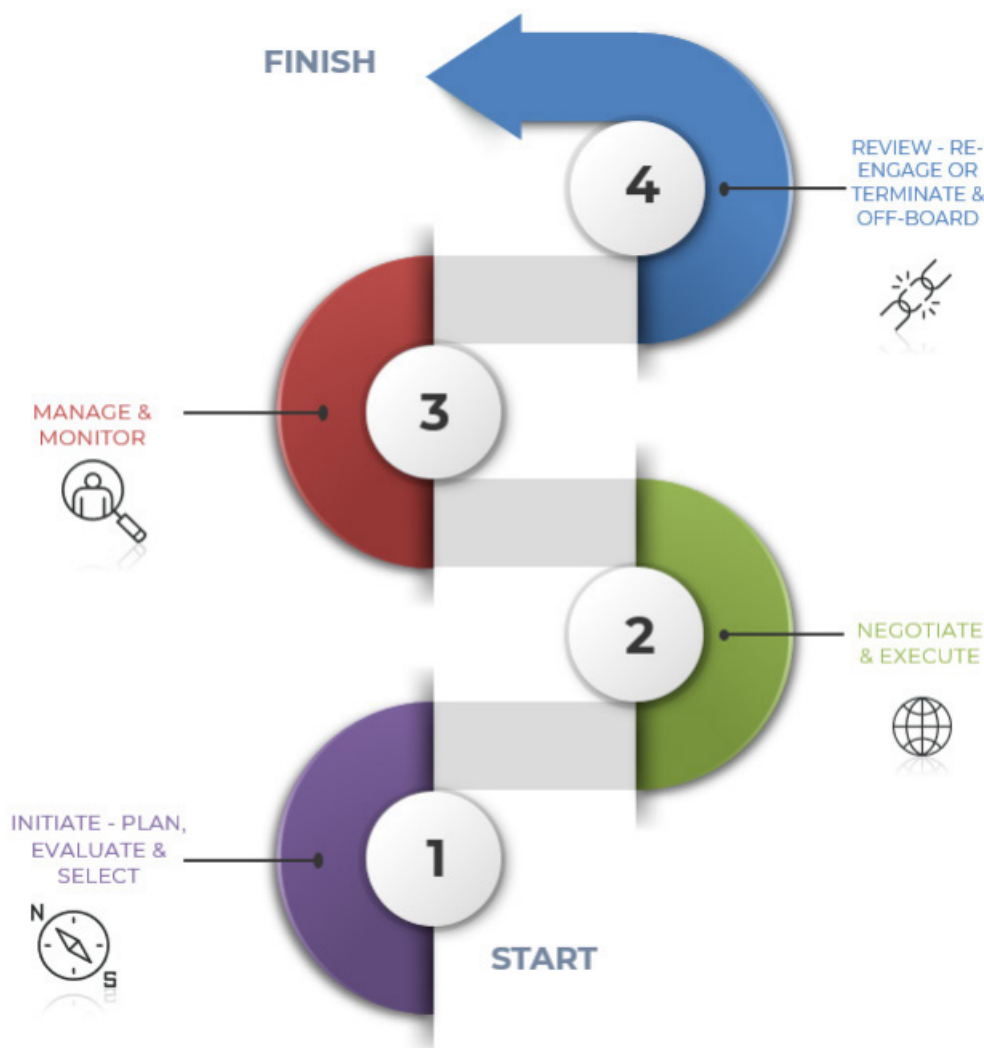
2. Changes to critical and high-risk third-party arrangements

2.1.   This procedure applies to both the initial engagement and any subsequent changes to critical and high-risk third-party arrangements, including where:

- an existing critical or high-risk third-party arrangement will be changed in a significant way (e.g. a major change to scope/price/subject matter or a new third-party will be added to the arrangement)
- a new sub-project will be initiated under an existing third-party arrangement that is currently not critical or high-risk, but the new sub-project is assessed as critical or high-risk.

3. Controls for critical and high-risk third-party arrangements

3.1.   All critical and high-risk third-party arrangements must follow the four-stage lifecycle:

3.2. The four stages must be completed sequentially. The [Third-party Arrangements Manual](#) contains an explanation of each stage and the steps required for completion.

4. Reporting of critical and high-risk third-party arrangements

4.1. The Risk Management team will annually report the central register of critical and high-risk rated commercial activities with third parties to the ULT and the Safety and Risk Committee of Council.

4.2. Local areas must report annually, or on request, all critical and high-risk rated commercial activities with third parties to the [Risk Management team](#).

Section 3: Records of third-party arrangements

1. All third-party arrangements

1.1. Records must be kept of all third-party arrangements (not just those that are critical and high-risk).

1.2. Faculties, schools, divisions, business units or centres (the **local areas**) must store their third-party arrangements in line with UNSW's [Recordkeeping Policy](#) and [Recordkeeping Standard](#).

1.3. Local areas must store all records relating to their third-party arrangements in line with [UNSW Systems of Record](#). This includes:

- the fully executed copy of the agreement; or
- any other document capturing the arrangement.

1.4.   Local areas must record the following for a third-party arrangement:

- a brief description of the subject matter
- details of the parties involved
- date of execution and expiry of the arrangement (including options to extend the term)
- total funds to be paid by either party over the life of the arrangement
- date of approval of the arrangement and date when it will be reviewed
- details of any appointment by or on behalf of UNSW to relevant boards or other governing bodies
- details of any meetings where matters were considered and approved for complying with this policy.

1.5.   Local areas can contact the Records team within Records & Archives for any questions on storing records.

2. Critical and high-risk third-party arrangements

2.1.   The requirements outlined in sub-sections 1 and 2 of this procedure apply to storing critical and high-risk third-party arrangements.

2.2.   Local areas must ensure that records are saved in UNSW's records and archives management system (RAMS) using the classification:

- critical & high-risk arrangements with third parties
- university commercial activity (where the arrangement involves UNSW performing commercial functions).

2.3.   Sub-section 2.2 enables UNSW to comply with its obligations in:

- storing critical risk, high-risk and high value records in line with UNSW's Recordkeeping Standard
- maintaining a register of commercial activities in line with *section 20C of the University of New South Wales Act* 1989 (NSW).

3. Third-party arrangements worth $150,000 or more

3.1.   Copies of any agreements with private sector entities worth $150,000 (including GST) or more must be provided to Strategic Procurement for inclusion in UNSW's Government Contracts Register.

3.2.   Sub-section 3.1 applies to all third-party arrangements (not just those that are critical and high-risk).

3.3.   Legal & Compliance, UNSW IT and Estate Management can directly load copies of their agreements into the system provided by Strategic Procurement (refer to section 4.20 in the Procurement Procedure). This will ensure UNSW complies with its obligations under the *Government Information (Public Access) Act 2009* (NSW).

Section 4: Roles and responsibilities

1. UNSW Council

1.1.   UNSW Council fulfills its obligations in managing risk of third-party arrangements in line with the *University of New South Wales Act* 1989 (NSW).

2. Safety and Risk Committee of Council

2.1.   The Safety and Risk Committee of Council fulfills its obligations in managing risk of third-party arrangements in line with their Terms of Reference.

3. Senior leaders

3.1.   Senior leaders (e.g. Provost, Deputy Vice-Chancellors, Vice-Presidents, Deans, Chief Officers, Directors, Heads of School/department/unit):

- report annually, or as requested, all critical and high-risk third-party arrangements in their areas to the Risk Management team
- ensure processes are in place to assess third-party arrangements and for implementing the additional controls in arrangements that are critical and high-risk
- oversee the operation of this policy and third-party arrangements procedures within their areas of responsibility
- provide feedback on this policy to the Director of Risk.

4. Risk Management team

4.1.   The Risk Management team:

- implements the third-party arrangements procedures in this policy
- communicates this policy and the third-party arrangements procedures to UNSW staff and controlled entities
- supports local areas with the risk level assessment of a third-party arrangement
- engages with local areas to be aware of and keeps a record of all third-party arrangements, especially those that are critical and high-risk
- maintains a central register of critical and high-risk rated commercial activities with third parties
- reports critical and high-risk third-party arrangements annually to the ULT and the Safety and Risk Committee of Council
- reports to the Vice-Chancellor or members of the ULT all critical and high-risk third-party arrangements as requested.

5. Staff

5.1.   Staff that perform operational activities:

- report and escalate to their supervisor any critical and high-risk third-party arrangements that have been identified
- follow defined processes, activities and controls for third-party arrangements.

Effective: 1 June 2024   **Responsible:** DVC TPA   **Lead:** Director of Risk

Appendix 1: Roles, responsibilities and legislative compliance

Authority for procedures and instructions

The following UNSW officers are authorised to maintain and change the procedure sections of this policy in line with the Policy Framework Policy:

1. The Deputy Vice-Chancellor Transformation Planning and Assurance (DVC TPA) has authority to approve a standard or procedure section of this policy.

2. The Director of Risk has authority to change
   - Risk Management procedures
   - Risk Management Manual
   - Third-party arrangements procedures
   - Third-party Arrangements Manual.

3. The General Counsel has authority to change:
   - Compliance Management procedures
   - Compliance Management Instructions.

4. The Head of Compliance & Privacy Law has authority to change the Compliance Management Instructions.

Responsibilities

5. The Director of Risk may approve the following to support this policy:
   - risk management processes
   - third-party arrangements processes

6. The Head of Compliance & Privacy Law may approve compliance management processes to support this policy

Legislative compliance

7. This policy supports:
   - the functions of UNSW Council in line with the *University of New South Wales Act* 1989 (NSW)
   - the effective management of obligations imposed by all legislation applicable to UNSW.