



Guidance Note

Governance and Risk Frameworks

This guidance material presents decision makers with a series of questions to evaluate their university's implementation of governance and risk frameworks in accordance with this pillar of the Guidelines to Counter Foreign Interference in the Australian University Sector. This material is advisory only. It provides specific considerations for decision makers to refer to as appropriate to their circumstances. The questions are grouped under themes to assist navigation.

Universities can manage their risks of foreign interference by:

- having an awareness of how foreign interference may occur
- determining the potential risks and consequences associated with university activities
- designating an accountably authority who is responsible for the university's mitigations
- developing policies and procedures which set out actions to mitigate risks
- instituting transparent escalation and reporting requirements.

Identifying acts of foreign interference

Examples of how foreign interference can occur include, but are not limited to:

- improper attempts to obtain information (such as sensitive or confidential information) from students or staff via foreign delegations, seminars, collaborations, or obligations of financial support
- inappropriately targeting and recruiting staff and students, including HDR students, to further a foreign actor's interests
- actions by or for a foreign actor that are inconsistent with academic freedom and the university's values or codes of conduct, such as demands or inducements to change academic programs for the benefit of a foreign political, religious or social agenda
- inappropriate efforts to alter or direct the university's research agenda into particular areas of research (this may occur through subtle forms of undue influence and engagement, and through funding arrangements that may also lead to a loss of future value and/or control of intellectual property)
- seeking inappropriate access to, or influence over, particular persons, areas of activity, or research outcomes through various forms of funding arrangements (e.g. donations) or collaborations, financial or other inducements targeted at individuals
- cyber targeting by exploiting network vulnerabilities and unauthorised access.

Identifying risks and consequences

Examples of risks of foreign interference for universities include:

- unwanted access and potential interference to research, sensitive or personal data
- loss of future partnerships / collaborations / talent attraction
- breach of legal obligations – contractual or legislative
- loss of intellectual property / commercialisation opportunity
- cultivation of the university community for information gathering
- undue influence of an agenda within or outside the classroom.

Examples of consequences of foreign interference risks include:

- damage to reputation – institution or researcher or research team
- loss of public or partner trust, credibility and integrity of research results or data
- loss of control over confidential data or findings, if another individual patents research outcomes, restricts access to it by other means
- loss of professional recognition of work / effort and career progression opportunities
- loss of potential revenue
- existing or potential partners may lose confidence in abilities to hold confidential information in the future
- ineligibility for future funding opportunities.

More serious activities can lead to sanctions, infringements, litigation or criminal charges. At their most serious, foreign interference activities can provide a pathway to espionage against Australia.

Accountable authorities

An accountable authority is a senior executive or executive body responsible and accountable for the security of people, information and assets to counter foreign interference. An accountable authority may be a:

- Deputy Vice-Chancellor
- Chief Information Security Officer
- suitably senior university staff member
- suitable senior university—level committee.

Universities and sector bodies could consider adding foreign interference as a standing agenda item or including it in Terms of Reference for existing executive/leadership/project groups.



Policies and procedures

Universities have a range of existing policies and procedures that support compliance with legislation and these may also be considered as part of managing foreign interference risks. Examples include, but are not limited to:


- sensitive research
- gifts and donations
- incident management
- ethical conduct in the workplace
- responsible conduct of research
- student codes of conduct
- staff codes of conduct
- complaints reporting and management
- anti-discrimination and freedom from bullying and harassment
- risk management procedures
- fraud and corruption control.

Universities can include elements in their policies and procedures to address conduct that could lead to foreign interference. Examples include, but are not limited to:

- protections in university codes of conduct for all students and staff from actions that contravene the codes, such as harassment and intimidation of individuals on campus, with codes of conduct publicly accessible to all students and staff.
 - alignment with codes on freedom of speech and academic freedom.
 - address activities such as doxxing or targeting individuals due to their academic contribution.
- consideration of issues particular to off campus, offshore and international delivery.
- managing claims of foreign interference sensitively, in line with university policies and taking account of confidentiality issues.
- mechanisms to protect individuals — both students and staff — from undue influence, harassment or intimidation, such as enabling the anonymisation of academic work and grading when engaging on sensitive topics.
- mechanisms that check a staff or student's understanding of foreign interference risk and mitigations prior to the university providing an individual with access to information and assets that may be at risk.

Escalation and reporting requirements

Effective reporting mechanisms help to facilitate information flow, communication of expectations, and identification of risks. Examples of escalation and reporting requirements include:

- internal audit schedules and reports
 - program review schedules and reports
 - annual reports
 - information security incident management reports
- 

- workplace grievances and complaints systems.

Templates or forms that guide staff will help consistency in reports on, for example, international collaborations, concerns or incidents of harassment, unauthorised access to data. Reporting provided to the accountable authority may address, for example:

- a summary of the incident
- those involved in the incident, including those affected and those who handled the incident
- detailed incident description, including any technical details
- response actions
- if or how the issues have been resolved
- lessons learnt.

