Australian Government
Department of Home Affairs

TechFIT
TECHNOLOGY FOREIGN INTERFERENCE TASKFORCE

Investee Due Diligence Guidance

Department of Home Affairs

Contact us

Enquiries regarding the licence and any use of this document are welcome at:
Technology Security Policy Branch
Department of Home Affairs
PO Box 25
BELCONNEN ACT 2616

Table of Contents

Overview

This document helps small-to-medium critical technology organisations ('investees') conduct due diligence on sources of investment for national security risks.

Investment allows Australian businesses to take advantage of global economic opportunities and drives growth locally. This investment is integral to the economy and gives Australians capital to research, procure, commercialise, and scale their businesses. However, in some cases, bad-faith investors have ulterior motives that present risks to Australian businesses and our national interest. These investors are targeting Australian organisations, and if successful, will damage your interests. Comprehensive due diligence is required to identify and reduce harms.

This guidance may be useful for organisations involved in the development, application, supply, procurement, financing or use of critical technologies. It may also be broadly useful for any organisation to conduct due diligence on an investment source.

It is vital organisations recognise the threat environment and uplift their security posture to protect themselves.

This document is not an exhaustive list of security concerns associated with investment sources, nor should it be used as the single source of investment risk management options. It is intended to be used in conjunction with other organisational risk management processes and documents, including the Foreign Ownership, Control, or Influence (FOCI) Risk Assessment Guidance.

The guidance component is divided into four sections:

1. Pre-investment considerations
2. Investee due diligence
3. Risk management
4. Post-investment considerations

The following sections provide key information to support the use of the guidance. This includes a Quick Reference Flowchart, Due Diligence Checklist, a list of resources (Appendix A) and Glossary (Appendix B).

The information collected during investee due diligence is point-in-time and should be reassessed throughout the investment lifecycle. Investment review should be considered on both a periodic and trigger basis. Triggers should include all relevant events which may change the risk complexion of an investment. For example, changes in ownership or structure of investment sources and broader geopolitical shifts.

The information provided does not constitute financial advice. You should consider seeking independent financial, legal, taxation, or other specialist advice to understand how the information in this document relates to your specific circumstances.

Quick Reference Flowchart: Simplified Investee Due Diligence Guidance

Step 1: Pre-investment considerations (p. 13)

- Have you considered your current security posture and identified your key strategic assets?
  - Yes.
  - No. Do not engage with investors.
- Have you considered your deal-breakers when it comes to investment sources or conditions?
  - Yes, go to step 2.
  - No. Do not engage with investors.

Step 2: Investee due diligence (p. 15)

- Request information from your investor and conduct due diligence activities. Consider factors which may not be immediately visible. You should consider:
  - Source of investment
  - Network of investment
  - Approach and behaviour of investment source
  - Conditions and attachments to investment

Step 3: Risk management treatments (p. 23)

- Following due diligence activities, you can make **risk-based decisions** to ensure your security.

Avoid	Manage	Accept
Risks that cannot be adequately managed.	Risks that require further controls to reduce likelihood and impact.	Risks that are within your appetite.

Step 4: Post-investment considerations (p.24)

- Have you considered what information, access or influence you will give the investor?
- Have you considered how you would enforce contracts if relying on an overseas jurisdiction?

Step 5: Plan for continuous review (p.25)

- Investors may appear to engage in good faith initially but subsequently change their behaviour and act or make requests outside agreed terms.
- Ongoing consideration and consistent review of bad-faith investor threats is critical.

Due Diligence Checklist

Note: The below Due Diligence Checklist has been developed to help investees conduct robust, point-in-time due diligence on prospective and current investments. It is not an exhaustive checklist, nor is it prescriptive. Organisations need to assess each investor independently and make a judgement as to whether the risk of accepting investment is within their risk appetite. To understand these due diligence activities in their full context, organisations are encouraged to read the entirety of this guidance.

Pre-investment risk management (pp. 13-14)	
You should strengthen your security posture, determine your risk appetite and define your risk management processes before seeking investment	
Identify the assets most critical to the success of your business – the assets, systems, and processes whose compromise would cause existential damage	☐
Restrict critical asset access to only the individuals or parts of your business who require it	☐
Create barriers – both physical and virtual – around each asset or system that is prioritised for protection	☐
Identify the roles that require access to sensitive information or critical capabilities and applied additional security screening and controls to them	☐
Establish a structured Security Awareness Training program which includes physical security, cyber and information security, insider threat risks, and other concepts as required by your organisation	☐
Establish a risk management program accountable to the board which can identify, assess, treat, and monitor potential risks which affect your organisation	☐
Identify a risk owner at the appropriate level who can lead and champion your security program across the business	☐
Understand the broader geopolitical, economic, and security environment that your business operates in, and how particular investment sources may introduce risk to this environment	☐
Check whether your business operates, researches, produces, or is part of the supply chain for a technology which is on the Critical Technologies in the National Interest List or whether the Defence and Strategic Goods List captures your goods, software or technology. • If so, you should consider what this means for your security responsibilities and how this will affect your investment strategy.	☐
Consider whether accepting certain investors would make you ineligible for other opportunities, such as Defence contracts	☐
Consider what your deal-breakers or redlines are when it comes to an investment	☐

Investee due diligence (pp. 15-22)

You should conduct thorough, repeatable, reviewable investment due diligence processes, even where there is time pressure on your investment decision.

Research your capital source and identify any Indicators of Concern	☐
Consider if your capital source could be compelled to share data or cooperate with a foreign government or its entities	☐
Consider the reputational risk that could be introduced by partnering with or receiving investment from the capital source	☐
Consider the commercial risk that could be introduced by partnering with or receiving investment from the investment source, such as the risk of IP theft	☐
Consider if an investor gains or is seeking to gain benefits other than financial returns	☐
Consider the capital structure of your investor, and if there is anything unusual or suspicious about this structure	☐
Consider the likelihood that the partner or investor could be susceptible to FOCI risks arising from members of their network	☐
Identify if a member of the network of capital has engaged in bad-faith investment activity previously	☐
Consider how you were identified and approached by a capital source, and if there were suspicious or unusual indicators during this approach	☐
Consider if the level of information or access the capital source is asking is suspicious or unusual • Has the investor asked for sensitive IP, technology, or knowledge, prior to any formal investment or partnership? • Has the investor signalled an interest or intent to influence decision-making or strategic direction through their investment?	☐
Consider if the amount of investment being proposed is suspicious or unusual	☐
Identify if the request includes unusual conditions, terms, or requests	☐
Consider whether the conditions or attachments to capital allow an investor to exert undue influence or control over company finances, technology, direction, or other aspects	☐
Consider whether the conditions would provide the investor with access to information or IP that would be detrimental to your business interests if shared with other parties	☐

Post-investment (pp. 24-25)	
You should consider and consistently review bad-faith investor threats to help protect your commercial viability and competitive advantage. Once identified, you should take appropriate risk management actions to protect your organisation	
Consider the information that is appropriate and necessary to share with investors	☐
Consider the level of access assigned to your investors and implementing corresponding access controls	☐
Consider how your investors store your information and the protections placed on information or IP • Organisations should consider implementing and exercising a contractual ability to audit your investors' security measures on a regular and ongoing basis	☐
Include provisions or conditions in your contractual investment documentation to protect key operations and data	☐
Consider how you would enforce your legal or contractual agreement if you had to rely on an overseas jurisdiction	☐
Establish governance and reporting structures that ensure your risk management strategy remains effective over time and in overseas jurisdictions	☐
Define the time and event-based triggers that will guide your ongoing review of investor due diligence	☐

Introduction

Australian organisations operate in a complex geopolitical, economic, and social environment. As outlined by the Director-General of Security in the *Australian Security Intelligence Organisation's (ASIO) 2025 Annual Threat Assessment*, Australians are **'facing multifaceted, merging, intersecting, concurrent and cascading threats.'**[1]

Australian organisations – including those developing critical technologies – must consider themselves a target for bad actors, and screen across a range of different vectors, including investment sources. Your business might not operate directly in the field of national security, but that does not mean that national security threats will not impact your business.

> **Bad-faith investors** do not have regard for your business interests. They will use equity ownership, collaboration, influence and access to the detriment of your commercial operations.
>
> Your intellectual property (IP) may be transferred; your competitive advantages may be lost; your supply chains may be compromised; and your reputation may be tarnished. Consider these risks as you conduct due diligence on current and prospective investors.

Recognising the security context you operate in, and tailoring your decision-making, will help protect your business and Australia's interests. These challenges are shared by our likeminded partners globally and require proactive risk management.

What is a bad-faith investor?

Bad-faith investors are organisations or individuals that deceptively invest in an organisation to cause immediate or future harm to that entity and to Australia's national or economic security. Foreign State-Owned Enterprises (SOE) and Private Owned Enterprises (POE), or entities linked to them, can use investments to gain ownership, control, or influence of Australian organisations. They are likely concerned with benefitting a foreign nation-state, to the detriment of Australian individuals, organisations, and our national security. This ownership, control, or influence can be damaging to the strategic or commercial interests of businesses, and our nation. Malicious control or influence can be gained from any size of investment, including minority holdings, and can appear from both Australian investors and foreign investors.

Note: The definition of bad-faith investors is specific to this guidance document only. For more information, please see Information Sheet on Bad-faith Investors.[2]

All organisations need to be aware of the risks posed by bad-faith investors; however, some sectors are at higher risk:

- **Critical technologies in the national interest:**[3] Innovation in key technologies will shape global outcomes for years to come and will see Australia collaborate closely with allies and likeminded partners. These technologies, which underpin our economic prosperity, national security, social cohesion, and our allies' interests, are likely targets for bad-faith investors. Some foreign governments have made clear their desire to prioritise these sectors for investment and technology transfer.

[1] Director-Generals Annual Threat Assessment 2025, Australian Security Intelligence Organisation, https://www.asio.gov.au/director-generals-annual-threat-assessment-2025
[2] Bad-faith Investors: Information Sheet, Department of Home Affairs, https://www.homeaffairs.gov.au/nat-security/files/info-sheet-bad-faith-investors.pdf
[3] List of Critical Technologies in the National Interest, Department of Industry, Science and Resources, https://www.industry.gov.au/publications/list-critical-technologies-national-interest

- **Dual-use and military technologies:** Technologies with both civilian, military and intelligence application are at higher risk because they can provide foreign powers with insights into Australia and our allies' capabilities and help strengthen their own. Bad-faith investors may operate under false pretences and hide their intent to use these technologies to advance their military capabilities. If you are unsure of the export control status of specific goods, software and technologies, check the Defence and Strategic Goods List or contact Defence Export Controls.[4]
- **Small-to-medium enterprises, including start-ups and spinouts:** These organisations may lack the resources and capability to conduct due diligence on sources of funding. Bad-faith investors may also use complex obfuscation techniques or place time pressure on these organisations to increase the likelihood that their investment will be accepted.

Be aware: Bad-faith investors may use investment for objectives other than financial returns.

Case Study 1: Secret side letters.

A technology start-up seeking investment to sustain operations engaged with a foreign venture capital firm. The foreign firm was registered in an offshore jurisdiction, while its principals and partners were based in a third country. This structure is commonly used in international venture financing but raised initial questions about transparency and governance.

The start-up received a term sheet from the foreign firm and shared it with existing investors. Upon review, investors noted the term sheet referenced a "side letter." The side letter contained provisions granting the foreign firm inspection rights and access to sensitive information, including IP details and the company's technical roadmap. Further examination revealed additional non-standard terms in the term sheet, such as an unusually high redemption premium far exceeding the principal amount, along with other atypical conditions.

The foreign investment firm exhibited several red flags:

- **Opaque ownership links:** Registration in an offshore jurisdiction combined with international principals.
- **Requests for sensitive IP access:** Inspection rights beyond standard investor protections.
- **Non-market terms:** Excessive redemption premium and unusual conditions.
- **Concealed agreements:** Use of a side letter to introduce terms not disclosed in the main agreement.

Through negotiation, the start-up successfully removed the most intrusive provisions from the side letter. However, due to financial necessity, it ultimately accepted the investment under revised terms.

Early due diligence and proactive engagement helped to mitigate risks and reduce material commercial impacts, such as loss of critical IP, limited future funding opportunities, or reduced valuation.

What is foreign ownership, control or influence (FOCI) risk?

FOCI risk refers to the ability for companies or shareholders to be directed by a foreign government, either through direct ownership channels, the domestic laws of a foreign jurisdiction or outside influence (such as political party membership) to conduct malicious activities on behalf of that government.[5]

[4] Defence and Strategic Goods List, Department of Defence, https://www.defence.gov.au/business-industry/exporting/export-controls-framework/defence-strategic-goods-list
[5] Foreign Ownership, Control or Influence (FOCI) Risk Assessment Guidance, Department of Home Affairs, https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/technology-and-data-security/foreign-ownership-control-or-influence-risk-assessment-guidance

The primary driver of FOCI, and a key indicator, is the existence of a permissive legal environment in the foreign jurisdiction.

Managing FOCI risk extends beyond national security; it encompasses protecting your organisation's reputation, systems and IP, your business interests, and the privacy of your staff and customers.

- **Foreign ownership:** foreign governments or entities holding direct or indirect ownership stakes, including through investors, subsidiaries, or parent companies.[6]
- **Foreign control:** foreign laws or governance arrangements that inform, coerce or interfere with decision-making processes and key aspects of a business, such as IP access.
- **Foreign (malign) influence:** coercive economic leverage, strategic partnerships, or even subtle political manoeuvring. Foreign threat actors may exert influence in a not transparent way, compounding risks.

Why is Australia a target?

Australia is an attractive target because of our position as a scientific and technological innovator and our strategic alliances with global partners. Organisations should not rely on Australia's strong economic and trade relationships to deter bad-faith investors acting on behalf of a foreign government. Some foreign governments have stated their intention to transfer technology and innovation from countries, including Australia, to supplement their own domestic industry and military capabilities.

> "A range of countries – some we consider friendly – have a relentless hunger for strategic advantage and an insatiable appetite for inside information.
>
> Most commonly, that manifests in the theft of privileged information about government decision-making, defence capabilities, and intellectual property or cutting edge-research, particularly if it has both military and civilian applications.
>
> Increasingly, though, foreign intelligence services are broadening their collection requirements. They are aggressively targeting private sector projects, negotiations and investments that might give foreign companies a commercial advantage…
>
> Foreign companies connected to intelligence services have sought to buy access to sensitive personal data sets; sought to buy land near sensitive military sites; and sought to collaborate with researchers developing sensitive technologies."
>
> Mike Burgess AM – Director-General of Security – 12 November 2025

Investment vehicles such as sovereign wealth funds and venture capital firms may be used to **support foreign espionage and interference** activities. These **activities include the unwanted transfer of technology** to gain or widen a technological edge.

[6] Venture Capital and Supply Chain Vulnerabilities, National Counterintelligence and Security Center, https://www.dni.gov/files/NCSC/documents/supplychain/Final%20VC.pdf

How are businesses harmed?

As critical technologies, supply chains, and critical infrastructure become more connected, the distinction between private business and broader national security is narrowing. Today, businesses are at the front line of geopolitics, and they are a target for bad-faith investors.

Decision-makers need to look more closely at the source country of investors and the networks around the source. The wide-ranging harms and business impacts from bad-faith investors can include:

Action	Harm Description	Business Impacts
Unwanted technology transfer	The transfer of, or communication about, a critical technology (such as trade secrets or IP), which may prejudice the security, defence, economy, or international relations of Australia, or an Australian business.[7]	Loss of competitive advantage Reputational damage Commercial damage Legal costs
Data exfiltration	The unauthorised or non-transparent transfer or exploitation of personal information, aggregate population data, organisational datasets and/or other data with value.	Loss of sensitive and personal information Loss of stakeholder trust Reputational damage Commercial damage Legal costs
Supply chain influence	The disruption, coercion, or influence of a supply chain or specific elements within or across it.	Loss of strategic or operational control Commercial damage, including to broader sector and economy Loss of trust in critical services and business operations
Sabotage	Any activity that damages, impairs or introduces a vulnerability to public infrastructure, including electronic systems, prejudicing Australia's national security or to advantage a foreign power.[8]	Increased downtime or loss of service Reputational damage Commercial damage Loss of trust in critical services and business operations
Undue influence and coercion for strategic or operational direction	Compulsion to act against the best interests of the business, or nation, in pursuit of an investor's commercial or strategic interests.	Loss of strategic or operational control Reputational damage Commercial damage

Organisations that partner with bad-faith investors may face additional scrutiny when seeking future funding or partnership opportunities, particularly within sensitive or highly regulated sectors. These harms are complex, damaging and cumulative. They can have significant and cascading effects on national security, business confidence, commercial viability, and the broader economy.

[7] Supplies of controlled technologies may be subject to Australia's export control legislation. Further information is available at Defence Export Controls.
[8] The Cost of Espionage, Australian Security Intelligence Organisation, https://www.asio.gov.au/system/files/2025-07/The%20Cost%20of%20Espionage%20Report%20July%202025.pdf

What is considered a trusted and secure investment source?

A **trusted** and **secure investor** is an entity independent from, and not susceptible to, foreign government direction, coercion, or pressure to engage in malign activities against Australia. This type of investor is more likely to:

- be headquartered in a democratic country with a strong rule of law, effective judiciary, transparent government processes, strong IP rights and private sector independence; and
- provide verifiable and transparent information regarding their ownership or investment structures and their motivations and intentions.

This extends to the investor's parent organisation or major investment sources.

Many democratic countries, including Australia, have legal provisions to compel entities to assist government with specific functions (for example, law enforcement activities). The Organisation for Economic Co-operation and Development (OECD) has developed broad criteria and principles by which government access to personal and sensitive data is managed.[9]

Why does jurisdiction matter?

Jurisdiction matters because some foreign governments have interests, values, and legal frameworks that do not align with Australia's, or those of our likeminded partners. These governments actively seek to collect large volumes of data, IP, research, and other sensitive information about Australia's critical assets and people. They are more likely to exploit companies to advance their strategic objectives, including through the malign and extrajudicial use of corporate entities to support espionage, sabotage and foreign interference activities.

Foreign laws

Some countries have laws that allow their government to leverage the resources and capabilities of any organisation or individual if deemed relevant to the country's interest. Such measures can include:

- Access to data and communications generated or stored by industry within the country
- Authority to collect, analyse, and retain all data transmitted across national networks
- Powers to inspect computer systems, require data localisation, and control online content

For example, China's National Intelligence Law (2017) enables Chinese intelligence and security agencies to require any organisation or individual to provide information, resources, or access where national security is concerned. This law applies to entities operating in China, Chinese citizens overseas, and may also be used to influence organisations with Chinese links, including subsidiaries and joint ventures.

Russia's System for Operational Investigative Activities law grants Russian security services the authority to collect, analyse, and store all data transmitted over Russian networks. Internet service providers are required to install monitoring equipment that enables the direct collection of network traffic.

Five Eyes

Australia, Canada, New Zealand, the United Kingdom, and the United States have a long history of diplomatic cooperation, coordination and information sharing on security and intelligence matters. This relationship is underpinned by shared values, respect for the rule of law, a high level of mutual trust, and a broadly similar geopolitical outlook, including common challenges and threats. Australian companies that engage with investors in Five Eyes countries are more likely to reduce exposure to bad-faith actors.

[9] Declaration on Government Access to Personal Data Held by Private Sector Entities, OECD Legal Instruments, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

Resources to assist organisations in considering jurisdictional hazard when assessing an investment source are available at Appendix A and in the FOCI Risk Assessment Guidance which includes indicators of heightened jurisdictional hazard, how to appropriately establish exposure, and how to rate FOCI risk.

Reviewing sources of investment

This section details the steps, considerations and information needed for investees to conduct due diligence on investment sources. It is intended to help organisations assess their exposure to bad-faith investors and FOCI risk. This guidance should be used in conjunction with other risk management processes and tools.

There are a range of resources and tools, including specific technologies, which can be used to conduct or support due diligence.

Note: The Australian Government does not provide guidance on specific tools and vendor solutions, including for due diligence. Each organisation should review available options and select the best option based on requirements, cost and risk profile.

Pre-investment risk management considerations

Organisations should strengthen their security posture, determine their risk appetite and define their risk management processes before seeking investment. Security risks accrued prior to or during an investment process could have significant long-term implications on an organisation's commercial interests. Organisations should apply these considerations across all business areas and processes.

Considerations for businesses prior to seeking investment:

- Identifying the assets most critical to the success of your business – the assets, systems, and processes where compromise would cause existential damage.
    - This may include your organisation's sensitive IP, source code, physical assets, data, key personnel, know-how or methodology, unique research and customer lists.
- Restricting access to critical assets to only the individuals or parts of your business that require it. Consider the need-to-know and least privilege principles.
    - The need-to-know principle means people should only have access to sensitive information if they genuinely require it to perform their role (e.g., just because someone works at the organisation, does not mean they have a genuine need-to-know about certain information relating to the business).
    - The principle of least privilege means that people, systems and applications should only have the minimum level of access needed to perform their function, and nothing more.
- Placing barriers – both physical and virtual – around each asset or system that is prioritised for protection.
    - This should include use of security frameworks such as the Essential Eight[10] or the Information Security Manual.[11]
- Identifying the roles that require access to sensitive information or critical capabilities and applying additional security screening and controls to them.
- Establishing a structured Security Awareness Training program which includes physical security, cyber and information security, insider threat risks, and others as required by your organisation.

[10] Essential Eight, Australian Signals Directorate, https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/essential-eight
[11] Information Security Manual, Australian Signals Directorate, https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism

  - This program can be tailored to the level of information access granted to individuals, their system privileges and current or emerging threats.

- Establishing a risk management program appropriate to the size and complexity of your organisation and accountable to the management or ownership. This will help you more easily identify, assess, treat, and monitor organisational risks.
  - Organisations might consider the published Guidance for the Critical Infrastructure Risk Management Program. While the Guidance supports regulated, critical infrastructure entities to meet their regulatory obligations to have a risk management program, it may also be used by non-regulated organisations to develop and strengthen their risk management practices.
- Identifying a risk owner at the appropriate level who can lead your security program across the business.
  - The appropriate level for this person will differ for each organisation. Also consider reporting lines to ensure that identification or risks or issues by the risk owner can be escalated or advised to key management persons in a timely manner.
  - In smaller organisations this role may be assigned to someone completing other key roles or 'dual-hatting', such as the Chief Executive Officer or Chief Operating Officer. Security is an integral part of business success and viability no matter the size of the organisation.
- Acknowledging the broader geopolitical, economic and security environment that your business operates in.
  - Organisations should consider public attributions and international sanctions in place such as those on the Consolidated List of all persons and entities listed under Australian sanctions laws.
  - Public-facing national security materials, including Annual Threat Assessments from the Director General of ASIO are useful educational products.
- Considering whether your business operates, researches, produces, or is part of the supply chain for a technology which is on the Critical Technologies in the National Interest List[12] or whether the Defence and Strategic Goods List captures your goods, software or technology.[13]
  - If so, you should consider how this may impact your risk profile, pursuit of investment and the due diligence activities you conduct on investment sources.
- Determining whether accepting certain investors would make you ineligible for other opportunities, such as Defence contracts.
  - Identifying what your deal-breakers are when it comes to seeking investment.
  - Deal-breakers could include one or a combination of adverse investment terms, misaligned IP rights, opaque capital structures, links to high-risk jurisdictions or other terms your organisation is not willing to compromise on.

Case Study 2: Countering bad-faith investors in practice.

An Australian technology start-up was conducting a review of its investor base. The start-up identified a particular investor within its capitalisation table that was deemed high-risk due to the source of the investment.

To remove this high-risk investor, the company bought out this investor at the fair market price. Company leaders highlighted that this action was pursued as part of company business strategy and to best position the company for future growth in the current geopolitical climate.

[12] List of Critical Technologies in the National Interest, Department of Industry, Science and Resources, https://www.industry.gov.au/publications/list-critical-technologies-national-interest

[13] Defence and Strategic Goods List, Department of Defence, https://www.defence.gov.au/business-industry/exporting/export-controls-framework/defence-strategic-goods-list

Investee due diligence

Conducting due diligence as an investee can be challenging. Organisations are often under significant financial and time pressures. These pressures should not stop businesses conducting thorough, repeatable, reviewable investment due diligence processes. Failure to do so could compromise future commercial and reputational interests.

The following guidance outlines how investees can conduct due diligence to help manage bad-faith investors and FOCI risks.

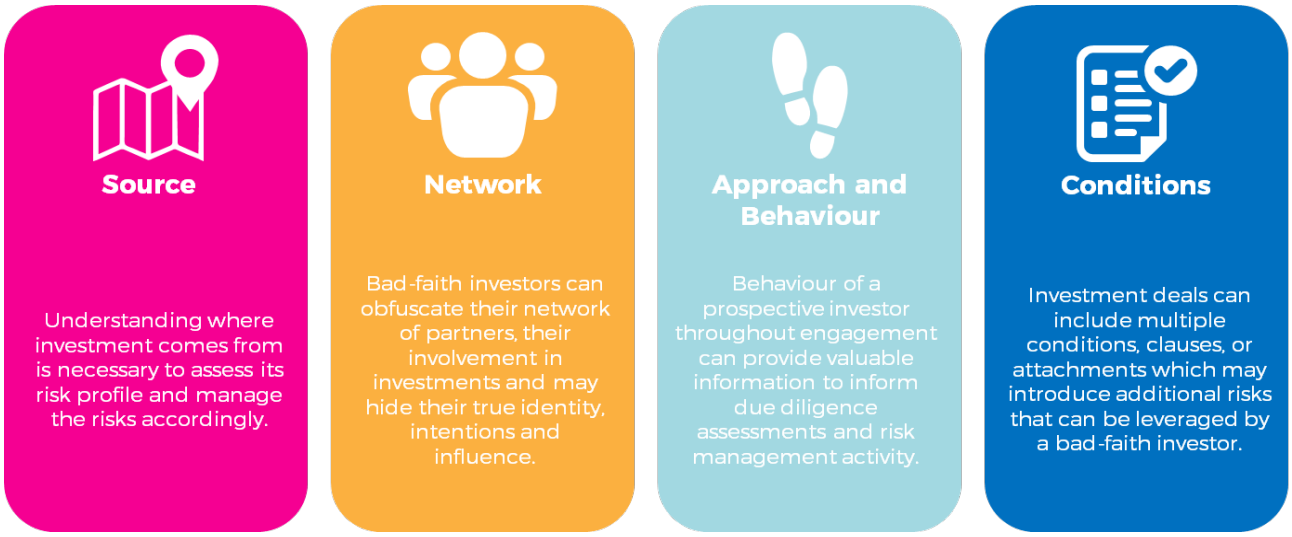

Figure 1: Investee due diligence

Source of investment

Identifying and verifying the direct source of capital investment should be your starting point. This helps organisations assess the investor's risk profile and manage any risks.

Information provided by investors should be carefully reviewed to confirm their identity and legitimacy, and cross-checked against reliable sources such as the Australian Securities & Investments Commission (ASIC) Company Register.[14] Organisations can draw on other publicly available information to identify the source of capital. For example, media reporting or likeminded government reporting on sanctions or other restrictions on an investor, their parent company or related entities. The Australian Transaction Reports and Analysis Centre (AUSTRAC) has published guidance regarding beneficial ownership and control structures[15].

Additional checks for information can be undertaken using online search tools, industry contacts, or open-source intelligence tools. Trusted third party providers can support the due diligence process by offering point-in-time and ongoing checks that streamline the process. See Appendix A for recommended resources.

Indicators of Concern (IoC) will help guide your due diligence process. The table below outlines IoCs to consider when assessing information about an investor's source of investment.

Note: This is not an exhaustive list of IoCs. An investor may display some IoCs without being a bad-faith investor. Organisations need to assess each investor independently and determine whether the risk of accepting investment is within their risk appetite.

[14] ASIC Registers, Australian Securities & Investments Commission, https://www.asic.gov.au/online-services/search-asic-registers/
[15] Determining ownership and control structures, Australian Transaction Reports and Analysis Centre, https://www.austrac.gov.au/industry-and-business/obligations-and-guidance/additional-guidance/determining-ownership-and-control-structures

Indicator of Concern	Indicator Description	Reasoning
Entities with a high level of jurisdictional hazard	Entities with the potential for increased risk due to differences in laws, regulations and political stability of a foreign nation. A list of indicators of heightened jurisdictional hazard is contained within the Foreign Ownership Control and Influence Risk Assessment Guidance.	Likely susceptible to political influence, interference and direction.
State-owned enterprises (SOE)	Enterprises which are majority owned by a foreign government authority (national or local) in nations with a high jurisdictional hazard.	Likely susceptible to political influence, interference, and direction.
Military or intelligence enterprises	Enterprises which are either direct functions of or partly owned by military or intelligence organisations in nations with a high jurisdictional hazard.	Likely susceptible to political influence, interference and direction. They are also more likely to seek a strategic advantage, such as increased control and influence, or access to information which enhances their capabilities in key areas.
Sovereign wealth funds (SWF)	State-owned investment fund or similar investment structure in nations with a high jurisdictional hazard.	Likely susceptible to political influence, interference and direction.
Links to influence operations	Influence operations are activities used to shape foreign environments for more favourable outcomes, often in exchange for significant investment in regional infrastructure or social initiatives. This includes talent programs, mis- or disinformation campaigns, or economic campaigns.	Likely susceptible to political influence, interference, and direction, especially those from nations with a high level of jurisdictional hazard.

Indicator of Concern	Indicator Description	Reasoning
Sanctioned entities[16]	Entities with restrictive measures imposed on them in response to a situation of international concern. Sanctions take many forms including financial sanctions, travel bans, trade sanctions and commercial activity sanctions.	Indicates a higher level of inherent risk potentially due to strong links to state-owned entities, military entities or intelligence entities.
Export control violations	Entities that have violated export controls in the past, either in Australia or other geographies with similar export control regimes and goals to Australia.	Indicates a willingness to defy laws and regulations for their own benefit and strategic aims. It can also indicate the broader malicious intent of a bad-faith investor.
Complex capital structures	Ownership and control structures which are complicated, sometimes containing multiple layers, entities and geographic spread.	Whilst complex structures are commonplace, they make it more difficult to assess intention, capability, and strategic objectives of bad-faith investors. Complex structures can be indicative of an intention to obfuscate true ownership.
Poor or damaged public reputation	Entities with a poor public reputation, particularly with prior evidence or demonstrated intent to engage in malicious behaviour, including technology transfer, data exfiltration, criminal activity and other flagrant or high-risk activities.	Indicates a prior capability or intent to break legal contracts or engage in high-risk behaviour.

Considerations for businesses when assessing the investment source:

- Identifying the IoCs present for the investment source.
    - You should determine the impacts to your investment risk profile from these IoCs and whether they are significant enough to prevent your organisation from accepting investment.
- Whether the investment source could be compelled to influence your organisation to use certain vendors, share data or cooperate with a foreign state.
    - This may introduce commercial risks such as IP theft or sabotage.
- The reputational risk that could be introduced by partnering with or receiving investment from the investment source.

[16] OpenSanctions, https://www.opensanctions.org/

- Whether the investor is seeking, or would benefit from, non-financial benefits such as reputational gain or legitimacy within the market.
    - There are bad-faith investors who will use investment for objectives other than financial returns. Reputational benefits and legitimacy can be given to partners by obtaining access to additional business opportunities or corporate events. It may also help broaden the investor's network, including with government representatives, or access to experts.

Network of investment

Modern capital networks span across countries, currencies, markets and supply chains. Australia's trade links and innovation environment have created and promoted opportunities for many types of investment in local businesses. Bad-faith investors can use these complex networks to obfuscate their involvement in investments or hide their identity, intentions or influence. This can be through intermediaries or other methods.

Investees need to apply the same considerations, risk treatments and assessment process to the network of capital as they do to a direct source of capital. This includes minority investors, parent organisations, silent partners, key executives, directors or persons of influence, and any other individuals and groups that your business deems appropriate.

Be aware: bad-faith investors may obfuscate key details of their identity or networks to hide certain links, sources or beneficiaries.

Considerations for businesses when assessing an investment network:

- Seeking additional information from your investor which details their networks.
    - Taking additional steps to verify information provided – as highlighted in investment source due diligence.
- Identifying the capital structure of your investor to determine if there is anything unusual or suspicious within it.
    - Bad-faith investors may look to obfuscate parent organisations, beneficial owners, silent partners, key executive, director or person of influence details, or other key details to hide specific links. It is important for business to consider these risks and challenge their investors for accurate and verifiable information.
- The likelihood that the partner or investor could be susceptible to FOCI risks from a member of their network.
- Whether a member of the network of capital has engaged in bad-faith investment activity previously.

Approach and behaviour of investment source

Organisations should consider how they have been approached and the behaviour of an investor. Some investor behaviours will be considered standard business practice in isolation, but when collated together, they could indicate a higher security risk. You should scrutinise the behaviour of investors objectively, regardless of the investment terms offered.

When raising capital from multiple investors in a round, bad-faith investors may stand out.

The table below outlines Behaviours of Concern (BoC) which organisations should consider when conducting due diligence.

Note: This is not an exhaustive list of BoCs, nor is it prescriptive. An investor may display some of these BoCs without being a bad-faith investor or display none of the BoCs and be a bad-faith investor. Businesses need to assess each investor independently and make a judgement as to whether the risk of accepting investment is within their risk appetite.

Behaviour of concern	Behaviour description	Reasoning
Suspicious approach or engagement	Suspicious approaches or engagements could include: • Unsolicited business proposals, joint ventures, partnerships or investment opportunities • Proposals or investment opportunities which seem 'too good to be true' • Proposals or investment opportunities from intermediaries who do not disclose the beneficial owner of an opportunity • Approaches or engagement through social media, networking sites, cold calls, industry events, conferences or encrypted messaging applications • Approaches or requests for access or information when hosting foreign delegations or visitors.	May suggest increased risk from the investor and necessitates more fulsome due diligence.
Unusual requests	Unusual requests could include asking for: • Proprietary or sensitive information in pitch decks, reports, or other documents provided • Specifics around customer details, such as full lists, contractual amounts, project information and future pipeline (particularly if these include government, military or intelligence contracts) • Introductions to specific sensitive or high-value personnel • A briefing on sensitive topics, projects, research and information • A briefing on one topic and then switching the conversation to a different topic to discuss more sensitive topics, projects, research and information.	May suggest increased risk from the investor and necessitates more fulsome due diligence.
False or misleading information	Information provided turns out to be false or intentionally misrepresentative during or upon completion of due diligence.	May suggest that the investor is making a concerted effort to obfuscate their true identify or key information which may expose investor risks.

Behaviour of concern	Behaviour description	Reasoning
High pressure tactics	Tactics to create a sense of urgency to rush the business to complete their due diligence checks without adequate consideration of information. These tactics can include: • Setting short timeframes and deadlines • Caveating investment or partnership on the proviso that it occurs on their timeframe • Displaying aggressive, manipulative, or coercive behaviours.	May suggest that the investor is attempting to rush into a formal agreement and circumvent proper due diligence processes.
Sudden purchasing power or business activity	Displays or has a large amount of capital for investment or becomes highly active after a sustained period of inactivity.	May suggest the investor has a new source or network of capital. This new information would need to be interrogated as part of due diligence.
Lack of prior investment history within your sector	Displays a sudden change in investment strategy.	May suggest that the investor has a new motive and underlying intentions for investment. These may not align with your values or interests.
Lack of due diligence (from an investor)	Appears to rush the investment process without conducting appropriate due diligence on your business.	May suggest that the investor is attempting to rush into a formal agreement for reasons other than commercial gain.

Considerations for businesses when assessing investor approach and behaviour:

- How you were approached by an investor, and if there were suspicious or unusual indicators during this approach.
- The level of information or access the investor is requesting.
    - Whether the information or access is necessary for the investor. If it is suspicious or usual, you should seek further information on why it is required.
- Whether the investor has asked for sensitive information prior to any formal investment or partnership.
    - The investor may be based in a jurisdiction with laws or powers which would allow a foreign government to gain access to your IP, technology or data.
- What access and system controls you can use to protect your information if you ultimately decide to share the information requested.
- Whether the investor's behaviour suggests an interest or intent to influence decision-making or strategic direction through their investment.
    - This may include requesting to participate in board meetings, requesting board seats or that an executive of their choosing take a key position.

- Investments can begin with a minority share or board seat but increase this over time until they have meaningful control.

- If there is anything suspicious about the amount of investment being proposed.
  - An investment which far exceeds the market value may indicate malign intentions.
  - An unusual investment amount or structure may be an attempt to be circumvent legislative instruments or investment thresholds.

Conditions and attachments to investment

Investment partnerships can be complex. They often contain multiple parties, conditions, clauses and attachments to ensure the organisation and investor are meeting expectations. Investors often include different conditions to influence the strategic direction of an organisation, particularly those who focus on small-to-medium enterprises. This influence can allow investors to better protect their investment and drive the decision-making process in a way that aligns with their interests.

For bad-faith investors, this level of strategic influence can be catastrophic to the interests of a company. Influence over finance, customers, IP, technology stack, operational decisions, long-term strategic goals, and more, can leave your business exposed to significant risks.

Case Study 3: Don't let go.

In 2024, an Australian technology company went into voluntary administration after one of its investors made a series of decisions that made no commercial sense. These decisions included selling IP to a foreign corporation on terms highly unfavourable to the Australian company. This IP had commercial and military applications.

The table below outlines conditions or attachments to investment of concern which organisations should consider when conducting due diligence.

Note: This is not an exhaustive list of conditions or attachments to capital, nor is it prescriptive. An investor may request some of these conditions without being a bad-faith investor or not request any conditions and be a bad-faith investor. Organisations need to assess each investor independently and make a judgement as to whether the risk of accepting investment is within their risk appetite.

Condition or attachment of concern	Reasoning
Board seats	Board seats are a standard investment feature, particularly in start-ups. Board seats may warrant scrutiny where the investor seeks confidential information and voting rights that may unduly influence organisational strategy, management and policies.
Share options or rights	Share options, including the option to purchase further shares after a set period, are common investment terms. They become a concern where they enable a significant or rapid increase in ownership or control, or disproportionately influence governance relative to the investor's equity stake.
Executive, director, or employee placement	Placement of individuals within an organisation can allow bad-faith investors to gain strategic and operational information, as well as the ability to directly influence organisational activities.

Condition or attachment of concern	Reasoning
Vendor placement	Bad-faith investors may contractually require the use of certain vendors for direct commercial or strategic benefit, or to introduce supply chain vulnerabilities.
Access to physical locations, systems or information	Bad-faith investors may seek to gain access to physical locations, systems or certain information for the purpose of siphoning sensitive data or IP. This access may include foreign visitations or delegations. For example, an investor may seek to inspect a site, product, or technology.
Early or exclusive access	Investors may seek to gain early access or visibility of prototypes or fundamental research and products. Whilst this is normal for some investor relationships, bad-faith investors may use this access for malicious purposes. • The type of access and visibility is an important distinction. Investors may try to push the boundaries for purposes contrary to your business interests, for example by requesting access to physical prototypes or sensitive blueprints. This type of access or visibility is not typically required by normal investors and may suggest malicious intention.

Considerations for businesses when assessing conditions and attachments to capital:

- Whether the conditions or attachments to capital are suspicious or unusual in any way.
- Whether any data storage or access requirements in region with high jurisdictional hazard would expose a business to unwanted technology or data transfer risks.
- Whether the conditions or attachments to capital allow an investor to exert undue influence or control over company finances, technology, direction or other aspects.
- Whether the conditions would provide the investor with access to information and IP that would be detrimental to your business interests if shared with other parties.
    - Any physical, systems or information access provided should be tightly controlled. This includes preventing data exfiltration or any uncontrolled or unmonitored access from foreign jurisdictions.
    - Controls should apply if an investor is seeking early access to prototypes or fundamental research and development products.

Risk management

Following due diligence, appropriate risk management actions should be identified and applied in line with the level of risk assessed.

Organisations may have to make compromises to effectively manage the threat posed by bad-faith investors. This includes making trade-offs in the size and speed of an investment to ensure an investor is trusted and secure.

The below list details some of the strategies and controls that can be used to manage bad-faith investors. This is not an exhaustive list of risk management options or treatments, nor is it prescriptive.

AVOID THE RISK *Options to avoid risks that cannot be managed*	o **Denial and removal** – if bad-faith investor risk cannot be effectively managed, consider ceasing capital raising activity with that investor. If it is a current investor, consider removing them from your capitalisation table and remove their access or influence. o **Using a trusted investment source instead** – if available, you should use a trusted and secure investment source instead of a source with bad-faith investor risks. This could include a trusted domestic investment source, state, territory, or Australian Government investment vehicles, another investor on your capitalisation table or other investor options which you assess as trusted and secure.
MANAGE THE RISK *Controls to reduce likelihood and impact*	o **Technical controls** – scalable solutions to treat specific access and control risks. Refer to government advice such as the Protective Security Policy Framework,[17] Information Security Manual,[18] ASIO's Due Diligence Integrity Tool,[19] or other documents for specific guidance. o **Contractual controls** – the imposition of contractual obligations or provisions on an investor. For example, requiring adherence to stipulated risk management processes, requesting a mapping of their capital network, requiring that control, operations and data is kept within Australia, or requiring notification for any change of control, jurisdiction or key personnel changes. o **Administrative controls** – the reallocation of ownership or restructuring of capitalisation tables can allow you to reduce a prospective or current investor's ability for ownership, control, or influence. You should consider consulting your current investor base as well as trusted lenders to determine a practical approach. o **Engaging specialist legal, financial, or other advice** to thoroughly review the details of a proposed arrangement, condition, or attachment to capital. o **Monitoring and compliance regime –** as controls are implemented and risk is managed; organisations need to continually monitor their exposure and adjust controls accordingly.
ACCEPT THE RISK *Take no action and accept the risk*	o If there is risk associated with an investor, but they are within your risk appetite and can be managed, you may choose to take no further action.

[17] Protective Security Policy Framework, Department of Home Affairs, https://www.protectivesecurity.gov.au/
[18] Information Security Manual, Australian Signals Directorate, https://www.cyber.gov.au/business-government/asds-cyber-security-frameworks/ism
[19] Available on https://www.asio.gov.au/outreach

Post-investment considerations

Actions following the selection and approval of an investment source can be just as critical. Investors may appear to engage in good faith initially but subsequently change their behaviour and act or make requests outside agreed terms.

Ongoing consideration and consistent review of bad-faith investor threats is critical to help protect your commercial viability and competitive advantage. Once identified, it is up to you to take appropriate risk management actions to protect your organisation.

Investment review

You should undertake **time-based reviews** to assess the effectiveness of existing processes. Periodic reviews will ensure residual risks are minimised as the strategic and operating environment continues to evolve or when new information becomes apparent.

You should also undertake **event-based reviews** using triggers which may suggest a change in the risk profile of the capital. For example, changes in ownership or structure of investment sources and broader geopolitical shifts, such as updated sanctions listings or armed conflict events. This includes reviews as you grow and modify a product or service. As your technology matures, so too may your business sensitivity and risk profile.

Considerations for businesses after assessing a source of investment:

- Determining the information that is appropriate and necessary to share with investors post-investment.
- Determining the level of access to give to your investors post-investment and implementing corresponding access controls.
    - Organisations may also wish to consider restricting visitor access to sensitive areas to avoid the introduction of surveillance devices.
- Ensuring that your investors have placed protections on information and IP and data you share with them and confirming the effectiveness of these measures.
    - This could include provisions for timely and accurate reporting of incidents or contractual provisions to maintain the control of operations and data within Australia, and to require notification if an investor undergoes any change of personnel or jurisdiction.
- Confirming how you would enforce your legal or contractual agreement if you had to rely on an overseas jurisdiction.
    - There may be cases where this is impossible.
- Setting up governance and reporting structures that ensure your risk management strategy remains effective over time and in overseas jurisdictions.
    - These structures should include checks and audits for controls.
- Defining your ongoing time-based and event-based review processes. This should include time and event thresholds.
- Determining options for legal recourse to terminate investment contracts and obligations should significant risks be identified.

Hypothetical Case Study 1: Fast cash and no peer reviews.

Biotek-XYZ, an Australian biotechnology company, is conducting a capital raise to support its research and development activities.

During the capital raise they are approached by Crit-Tech Ventures, a foreign venture capital fund. Crit-Tech Ventures offer A$10 million for a 30 per cent share in Biotek-XYZ. This offer is significantly greater than any other offers from local firms and Biotek-XYZ needs capital to remain operational.

Biotek-XYZ conducts due diligence and uncovers that Crit-Tech Ventures has previously received investment from a foreign state-owned enterprise. They also find that a director from Crit-Tech Ventures has ties to the foreign country's military. Crit-Tech Ventures did not disclose the presence or links in their discussions.

Crit-Tech Ventures' term sheet is complex and lengthy. They are requesting direct access to sensitive IP and seek Biotek-XYZ to establish operations in their country with a director of their choosing. They are also requesting multiple board seats and share options.

Biotek-XYZ is concerned with some of these details and raises this with Crit-Tech Ventures. Crit-Tech Ventures threatens to withdraw their offer if it is not accepted within 72 hours.

Crit-Tech Ventures are displaying numerous indicators of concern:

- Obfuscation of foreign links and personnel details
- Disproportionate or 'too good to be true' offer
- Request for access to IP
- Request to place a director within the business
- Unreasonable contractual conditions
- Deadline to exert time pressure.

Biotek-XYZ should consider how they reduce their exposure by:

- Renegotiating terms to reduce undue influence, excessive access or unwanted IP transfer.
- Ceasing activity with this entity and exploring options with other investors.

While some of these facts in isolation are standard business practice, when considered together they indicate that Crit-Tech Ventures is likely a bad-faith investor. If Biotek-XYZ continues, they may be exposed to serious commercial and reputational risks, or even insolvency.

Let’s work together

As the strategic environment evolves bad-faith investors will continue to use capital as a vector to gain ownership, control or influence of Australian businesses and supply chains.

Australian entities should be attuned to the national and economic security risks that can affect their interests. This may differ from the way entities have viewed risk in the past. However, proactive efforts towards national security risk management will improve your entity’s resilience to potential commercial, reputational, and financial damages, and help support nation-wide economic resilience.

Effective investee due diligence within Australia requires cooperation between the Australian Government and industry.

Industry is strongly encouraged to share information relating to suspected bad-faith investors with the Australian Government. This information underpins the government’s understanding of the scale and scope of the threat across the economy and enables the delivery of effective advice and policy responses to counter bad-faith investors.

This information-sharing complements the government’s formal regulatory and screening framework for foreign investment. The Australian Government reviews transactions or arrangements that are subject to legislative frameworks, such as the *Foreign Acquisitions and Takeovers Act 1975* (FATA). Under the FATA, foreign investors are required to notify the Treasurer of a proposed investment if it meets the relevant requirements for screening.[20]

If you have concerns regarding suspicious or unusual activity related to espionage, sabotage or foreign interference, please contact your organisation’s security manager or advisor in the first instance.

You may also wish to report this directly to the National Security Hotline on 1800 123 400 or through the NITRO (Notifiable Incidents, Threats or Reportable Observations) Portal.

[20] Foreign Investment Portal, Treasury, https://investors.foreigninvestment.gov.au/

Appendix A – Resources

Resource & link	Further information
Resources on and guidance against threats to industry, critical infrastructure and academia	
• ASIO Outreach	• ASIO Outreach shares security intelligence with government and industry via a subscriber portal, briefings, and engagement. • The portal provides intelligence-backed insights on domestic and international threats. • ASIO protective security guidance, including the Secure Innovation campaign with Five Eyes partners, helps organisations manage security risks.
• Australian Signals Directorate's (ASD) Australian Cyber Security Centre (ACSC)	• ASD's ACSC delivers technical cyber security advice to strengthen Australia's cyber resilience. • The ACSC supports governments, businesses, and individuals with cyber security advice. • ACSC website provides cyber security guidance and programs, including the Strategies to Mitigate Cyber Security Incidents and the Australian Government Information Security Manual. • ASD's Annual Cyber Threat Report provides an overview of threats and advice for individuals and organisations.
• Department of Home Affairs: Critical Infrastructure Security Centre (CISC)	• CISC leads an all-hazards critical infrastructure regime with government and industry partners. • It supports critical infrastructure owners and operators to understand risks and meet regulatory requirements. • The CISC's Critical Infrastructure Annual Risk Review summarises security risks relating to Australia's critical infrastructure.
• Department of Home Affairs: Technology Foreign Interference Taskforce (TechFIT)	• TechFIT connects government and industry to protect Australia's technology, IP and innovation. • Due Diligence Resource Summary providing industry a list of resources on foreign interference and espionage-related matters. Factsheet for Critical Technology Sectors outlining outlines foreign interference and espionage risks, impacts, and mitigation options. • TechFIT are a 'front door' for foreign interference matters for industry. Email TechFIT@homeaffairs.gov.au.
• Department of Home Affairs: Foreign Ownership, Control or Influence (FOCI) Risk Assessment Guidance	• FOCI Risk Assessment Guidance helps organisations assess foreign ownership, control or influence risks when procuring technology.

Resource & link	Further information
	• It provides a repeatable template to support vendor due diligence and risk mitigation within procurement processes.
• Department of Home Affairs: FOCI Model Clause Bank for Australian Government Entities	• FOCI model clause bank equips Australian Government entities to manage and mitigate FOCI risks in procurement.
• Department of Home Affairs: Countering Foreign Interference in Australia Report	• The Countering Foreign Interference in Australia Report outlines key foreign interference risks and practical steps for organisations to address them.
• IP Australia: First Response	• IP Australia's tool and resources to help organisations manage IP related queries and risks, including IP infringement.
Resources for financial and investor due diligence	
• Australian Securities and Investment Commission (ASIC): Business Register	• ASIC registers provide a searchable database of registered business names and other relevant information.
• Australian Tax Office (ATO): Australian Business Register	• The Australian Business Register is a database of publicly available information supplied by businesses when they register for an Australian Business Number.
• Australian Transaction Reports and Analysis Centre (AUSTRAC): Politically exposed persons guidance	• A guidance document which can help identify politically exposed persons, and the risks and indicators of suspicious behaviour associated with illicit activity.
• AUSTRAC: Beneficial owners guidance	• A guidance document which can help identify beneficial owners where structures are complex.
• Treasury: Foreign Investment Guidance	• Treasury has a number of guidance documents available to help foreign investors understand their obligations under Australia's foreign investment laws and regulations.
• US Government: Safeguarding our innovation	• A threat awareness document which details foreign threat actors and potential indicators of bad-faith foreign investors.

Resource & link	Further information
• Browser search – 'open-source business intelligence tool'	• This search can identify tools which can be used to understand more information about a prospective or current investor.
Resources for geopolitical information, including public attributions and international sanctions	
• Department of Foreign Affairs and Trade (DFAT): Consolidated List	• The Consolidated List is a list of all persons and entities listed under Australian sanctions laws. • The Australian Sanctions Office (ASO) maintains the Consolidated List and updates it regularly. You can subscribe to their email list to receive updates.
• DFAT: Sanctions Risk Assessment Tool	• The Sanctions Risk Assessment Tool helps regulated entities conduct a preliminary assessment of sanctions risks. • It is guidance only, not legal advice, and should be used as part of ongoing compliance and due diligence activities.
• DFAT: Sanctions Guidance Notes	• The ASO advises across sanctions frameworks, including issues affecting multiple sectors and industries.
• Open Sanctions	• Open Sanctions is an international database of persons and companies of political, criminal or economic interest.
Cyber attribution and security information	
• ASD's ACSC	• The ACSC publishes a variety of alerts, advisories, and attributions which detail how foreign nations may present cyber security risks to Australian organisations.
Business risk information	
• UK Government: Overseas Business Risk collection	• The UK Government provides country-specific guides for UK businesses on political, economic and security risks when trading overseas.
• US Government: 2025 Investment Climate Statements	• The US Department of State's Investment Climate Statements help US companies make informed business decisions by providing up-to-date information on the investment climates of more than 170 countries and economies.
• US Government: Special 301 Report – Intellectual Property Protection	• The Special 301 Report is the US Government's annual review of global IP protection and enforcement. • It highlights key IP-related risks that hinder innovation and investment, including weak enforcement, trade secret theft, piracy, counterfeiting, and market access barriers.

Resource & link	Further information
Geopolitical information	
• ASIO: Director-General of Security's Annual Threat Assessment	• Key speech delivered by the Director-General of ASIO outlining Australia's current and emerging security threats.
• Australian Institute of Criminology: Cost of Espionage Report	• A report that quantifies the costs of espionage, both actual and prevented.
• Australian Strategic Policy Institute (ASPI)	• ASPI is an independent, non-partisan think tank that provides advice for Australian and global leaders and policy makers. • ASPI contributes to public discussion of strategic policy issues in the Indo-Pacific region on strategic, national security, cyber, technology and foreign interference issues.
• Lowy Institute	• The Lowy Institute is an independent, nonpartisan international policy think tank that conducts research regarding international political, strategic and economic issues from an Australian perspective.

Appendix B – Glossary

Note: The terms defined within this document are specific to this guidance document only.

Term	Definition
Bad-faith investor	Companies or individuals that deceptively invest in your company to cause immediate or future harm to an entity and to Australia's national or economic security.
Beneficial owner	An individual or persons who ultimately own or control an interest in a legal entity or arrangement, such as a company, a trust, or a foundation. Ownership and control may be direct (such as through shares) or indirect (such as shares held by a third party on the individual's behalf). 'Control' means having the ability to determine decisions about the entity's financial and operating policies.
Bulk data exfiltration	The unauthorised or non-transparent transfer or exploitation of personally identifiable information and company datasets and other data with value by companies, governments, or individuals.
Espionage	Theft of information or capabilities by someone either acting on behalf of, or intending to provide information to, a foreign power or foreign political organisation, that will prejudice Australia's national security or advantage the national security of a foreign country. Espionage can target defence, political, industrial, foreign relations, commercial, or other information or things that are usually unavailable to the foreign power.
Extrajudicial direction	A direction issued by an actor outside of, or without the permission of, the official legal system or legislation within the relevant jurisdiction.
Extraterritorial direction	A direction issued in the situation when a country extends its legal power beyond its territorial boundaries.
Five Eyes partners or countries	An alliance of five democratic countries who engage in mutual data and intelligence sharing and cooperate in areas of national security. This alliance includes Australia, Canada, New Zealand, the United Kingdom, and the United States.
Foreign interference	Activities carried out by, or on behalf of, are directed or subsidised by, or are undertaken in active collaboration with, a foreign power and either involves a threat to a person, or is clandestine or deceptive and is detrimental to the Australia's interests.
Foreign Ownership, Control, or Influence (FOCI)	An entity is considered to be operating under FOCI when a foreign interest has the power, direct or indirect whether or not exercised, and whether or not exercisable, through the ownership of the company under the purview of its National Security Authority/Designated Security Authority, by contractual arrangements or other means, to direct or decide matters affecting

Term	Definition
	the management or operations of that entity in a manner which may result in unauthorised access to classified information or adversely affect the performance of classified contracts or may otherwise be contrary to the interests of national security.
Intellectual property theft	The theft or unauthorised removal or movement of IP such as patents, copyrights, trademarks, trade secrets, or specific work products, from the rightful property holder. The theft may be intentional through malicious insiders or specific threat actors, or unintentional through human error.
Investee	A company, organisation, or person receiving investment from an investor. This guidance targets investees from small-to-medium critical technology organisations.
Least privilege principle	Personnel and services are granted the minimum access to systems (cyber supply chains, infrastructure, operating systems, applications and data) required to undertake their duties.
Need-to-know principle	The need-to-know principle reflects the need for personnel to only access information only where there is a requirement to do so to fulfil their duties. Limiting access by personnel (including contractors) to information on a need-to-know basis guards against the risk of unauthorised access or misuse of information. Personnel are not entitled to access information merely because it would be convenient for them to know or because of their status, position, rank or level of authorised access.
Sabotage	Any activity that damages, impairs or introduces a vulnerability to public infrastructure, including electronic systems, prejudicing Australia's national security or to advantage a foreign power.
Sanctions	Restrictive measures imposed on a particular individual, entity, country, group or vessel in response to a situation of international concern. Sanctions take many forms including targeted financial sanctions, travel bans, trade sanctions, and commercial activity sanctions. They may be designed to bring a situation of international concern to an end by influencing those responsible, to limit adverse impacts of a situation, or to penalise those responsible.
Threat actor	An individual, group or entity that intentionally performs malicious acts to compromise an individual or organisation.
Unwanted technology transfer	The transfer of, or communication about, a technology which may prejudice the security, defence, economy, or international relations of Australia or an Australian business. The transfer may be intentional through malicious insiders or specific threat actors, or unintentional through human error.

Term	Definition
Vector	A path, method, or means by which an attacker can break into a system, facility, or organisation.