Due Diligence Assessments

For Espionage and Foreign Interference Threats

PSR | Protective Security Requirements

Te Kāwanatanga o Aotearoa
New Zealand Government

This guide is to help you mitigate the risks associated with Foreign Interference. You can also adapt the approaches here to help mitigate reputational and other risks, including those coming from criminal activities or industrial espionage.

We developed this guidance with the UK's Centre for the Protection of National Infrastructure (CPNI), Business New Zealand, Universities New Zealand, Science New Zealand, New Zealand Trade and Enterprise (NZTE), NZ Growth Capital Partners, and Callaghan Innovation.

BusinessNZ

Science New Zealand

CPNI
Centre for the Protection of National Infrastructure

Te Pōkai Tara
Universities New Zealand

NZ GROWTH CAPITAL PARTNERS

CallaghanInnovation
New Zealand's Innovation Agency

NEW ZEALAND TRADE & ENTERPRISE
Te Taurapa Tūhono

PSR Protective Security Requirements

Contents

01

This guidance outlines potential Foreign Interference risks to New Zealand business, research, and investment. It has practical approaches to due diligence, including identifying and making informed decisions about potential risks.

Due diligence is a systematic assessment of the risks associated with any business, research, or investment decision with a new partner or collaborator. Due diligence also applies throughout the lifecycle of an existing business relationship, partnership, or investment.

In today's world of complex global relationships, we need to take care when doing due diligence. This care ensures that we encourage and keep harmless and innocent relationships. These relationships include economic, cultural, research, scientific, diplomatic, and political relationships.

WHO ARE YOU AT RISK FROM?

Foreign state actors target New Zealand businesses, organisations, and the research sector to steal personal data, research data, and intellectual property. These actors also try to access strategic assets using a range of methods, from espionage through to buying interests in businesses or their supply chains, or trying to become a part of an extended supply chain.

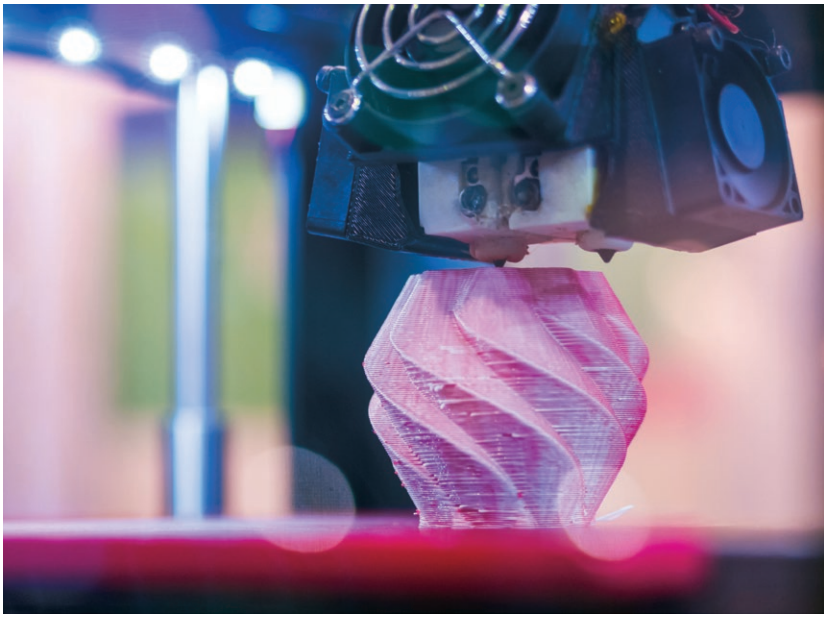
Possible reasons for this targeting include furthering military, economic, and technological interests. For example, international collaboration could offer foreign state actors the opportunity to benefit from research without carrying out traditional espionage or cyber compromise activities.

The opportunity to increase capabilities without the cost and uncertainty of research and development makes this an attractive option for some states.

Collaboration can provide access to people, IT networks, and participation in research and development that may be sensitive or have sensitive applications.

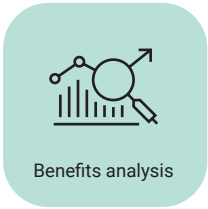
A foreign state actor's motive may be to:

- find opportunities to develop a research and innovation base that increases its economic, military, and technological advantages over other countries
- prioritise the stability of its regime and focus on suppressing internal dissent, political opposition, or media freedoms
- deploy its technological and security advantages against its own people to maintain the stability of the regime
- recruit offshore industry expertise to gain valuable capability and intellectual property, while reducing the capabilities of other state or enterprise competitors.



02 Due Diligence and Protective Security

New Zealand has an open economy, and conducts business and collaborates with individuals, businesses, organisations, universities, and researchers within New Zealand and internationally.



When entering any new partnership, risks need to be identified and managed to prevent damaged reputations, lost intellectual property (IP), or harm to New Zealand's national interests. Harm to our national interests includes harm to economic prosperity and resilience, international relations, or misalignment with New Zealand's broader policy settings.

Organisations and individuals considering domestic or international arrangements or collaborations do a range of things to evaluate the research, investment, or business opportunity and associated risks. This work includes assessing the benefits, considering ethical issues with the opportunity itself or the partner involved, reviewing IP management systems, and other considerations, in particular those related to national security.

While most business, investment, and research relationships will be assessed as providing an overall benefit, others may involve more risks, and need more consideration.

This evaluation process is called **due diligence**.

WHAT IS DUE DILIGENCE?

Due diligence:

- is a systematic assessment of the risks associated with any business, research or investment decision with a potential new partner or collaborator — it also applies throughout the lifecycle of a business relationship, partnership, or investment
- is a process that an individual or organisation can do using organisational records and readily available public information
- should be done repeatedly, be improved over time, and be embedded in systems
- allows decision-makers to factor into their decisions relevant risks, possible mitigations, and likely residual risk
- supports transparency and accountability.

The purpose of due diligence is to:

- avoid causing or contributing to adverse impacts on people, the environment, and society
- prevent adverse impacts directly linked to operations, products, or services through business or research relationships.

If adverse impacts cannot be avoided, due diligence should enable organisations to identify impacts in advance, mitigate them, prevent their recurrence and, where relevant, remediate them. (OECD Due Diligence Guidance For Responsible Business Conduct, 2018)

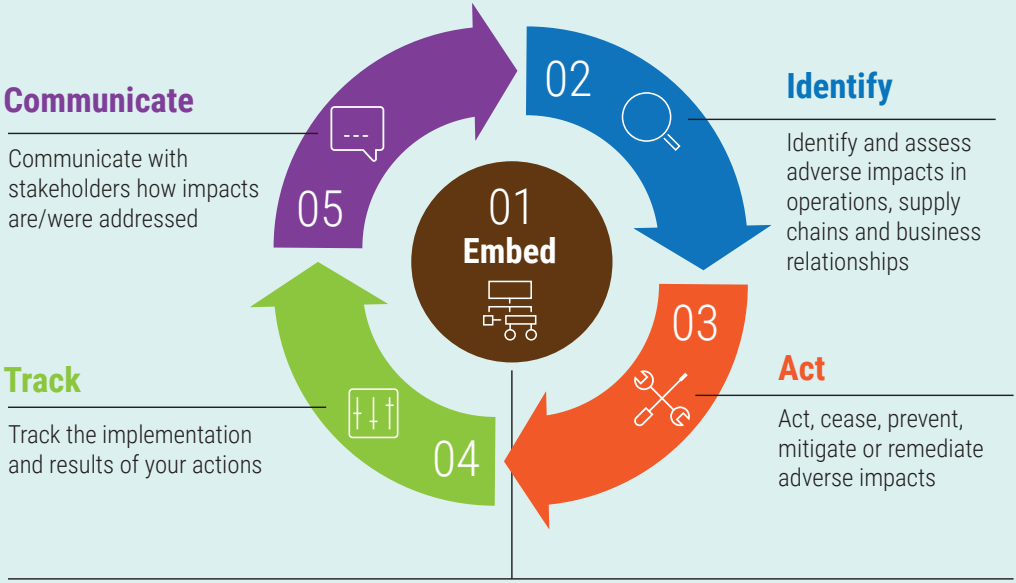
Increasingly, due diligence may include security considerations and other risks to national interest that may trigger regulatory systems or impact negatively on the reputation of an individual, organisation, or the nation itself.

Organisations should have a risk-management and decision-making framework to ensure an appropriate executive or board is responsible for the risk-management system. Decision-making can then be escalated to a level where approaches to risk can be decided.

03

Developing a system

Systems and processes should be documented to ensure consistent assessments and decision-making. These records should ensure the process is transparent, repeatable, and consistent.



Embedding responsible business conduct into policies and management systems is consistent with international best practice.

The degree of due diligence should be proportionate to the potential risks.

Collaborations with organisations and people from some countries can expose you to more risk. Countries that warrant greater scrutiny include those with poor human rights records, or where the government exerts considerable control over the private sector and civil society.

Be careful to avoid reputational risk associated with racial profiling or cultural stereotyping. This complexity arises, as countries are often associated with particular cultures and ethnic groups.

For lower-risk relationships, internet searches can reveal a great deal of useful information. This information is publicly and easily available online.

If you have a lot of international connections, you might want to develop some in-house capability to do due diligence.

Reports from international organisations, civil society organisations, national human rights institutions, government agencies, trade unions, and employer and business associations might have valuable information throughout the due diligence process, and particularly during the scoping phase. Media articles may also help you understand the local, regional, and national socio-political situation.

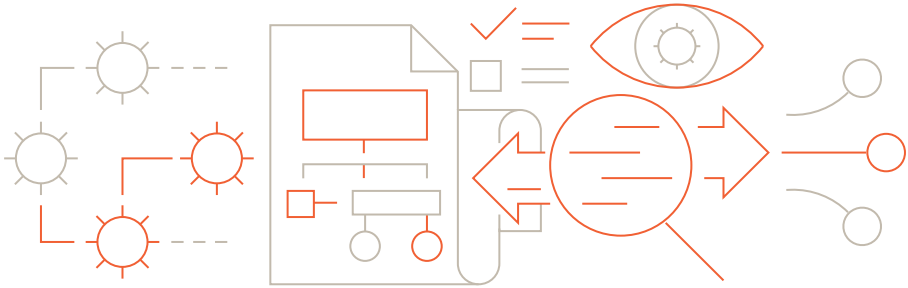
Foreign-language skills might be needed to do due diligence on some international partners.

Private companies can investigate and provide reports. These firms specialise in media scanning, corporate securities analysis, or other corporate risk services.

Many international relationships and research relationships are at a person-to-person or institution level. These relationships and common interests often go back years. Due diligence processes must be transparent and managed carefully to avoid creating suspicion and distrust that could damage these relationships.

Employees or researchers should ideally be involved in identifying risk since they are subject-matter experts directly involved in collaboration. Relying solely on external views may not fully capture the complex dynamics of collaboration and could distort the representation of risks.

Considerations



GOVERNANCE ARRANGEMENTS

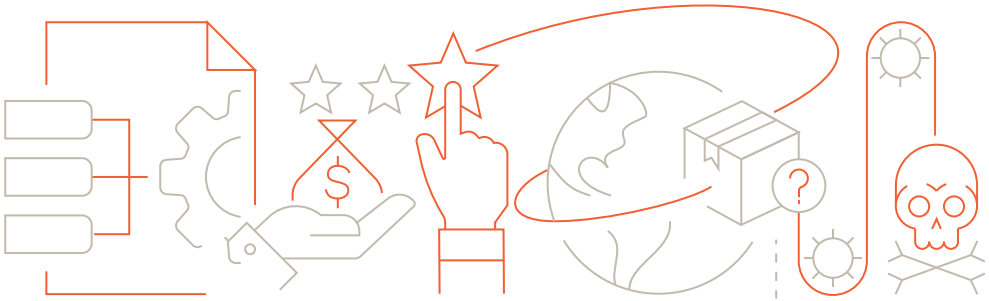
Organisations should document all policies and processes and record the outcome of considerations in a consistent way. This consistency will ensure that decision-making is transparent, internally consistent, and can be replicated. Review records regularly to ensure they stay effective and appropriate.

When identifying and assessing potential adverse impacts from supply chain and business relationships, you should develop escalation criteria and decision points where you must engage managers, senior executives, or boards.

These decisions could be based on a range of factors including the value of the transaction, reputational impacts, legislative requirements, or opportunity costs.

These governance arrangements will ensure:

- no surprises
- appropriate oversight
- decision-making occurs at appropriate levels
- consultation can occur with other business partners where required
- advice can be sought from government agencies.

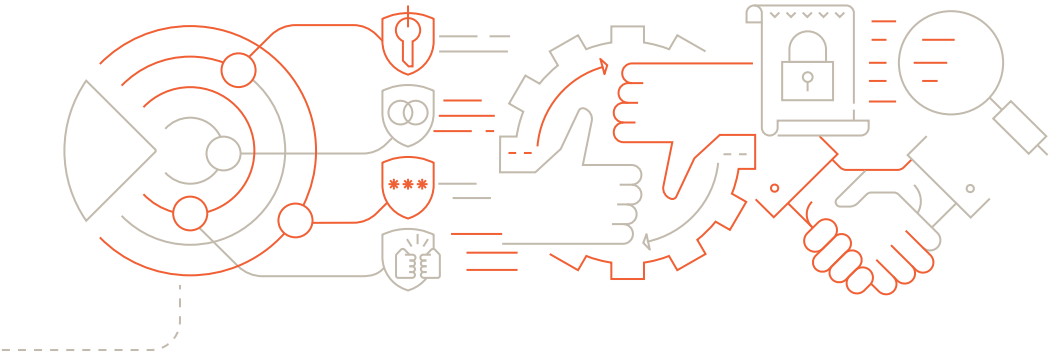


GOVERNMENT AND FUNDER REQUIREMENTS

Government and private funding and procurement processes increasingly require organisations to consider the risks associated with partners, collaborators, and the end use of any research or product.

Increasingly, the public and media also have expectations, and government procurers and research funders may need to consider reputational risks when making funding decisions.

An individual or organisation must meet the requirements of the New Zealand export controls regime. This regime is managed by the Ministry of Foreign Affairs and Trade and covers the export of military and dual-use goods and technologies, and exports to military, paramilitary, or police groups.



COLLABORATION

Collaboration is an important part of research and business. Most collaborations will not have any sensitive application and will not cause concern. Being clear on which areas of activity are sensitive is critical.

You can find specific advice on collaboration in research and academia in Trusted Research — Guidance for Institutions and Researchers at *https://www.protectivesecurity.govt.nz*

"The value and benefits of research are vitally dependent on the integrity of research. While there can be and are national and disciplinary differences in the way research is organized and conducted, there are also principles and professional responsibilities that are fundamental to the integrity of research wherever it is undertaken." (Singapore Statement on Research Integrity, 2010)

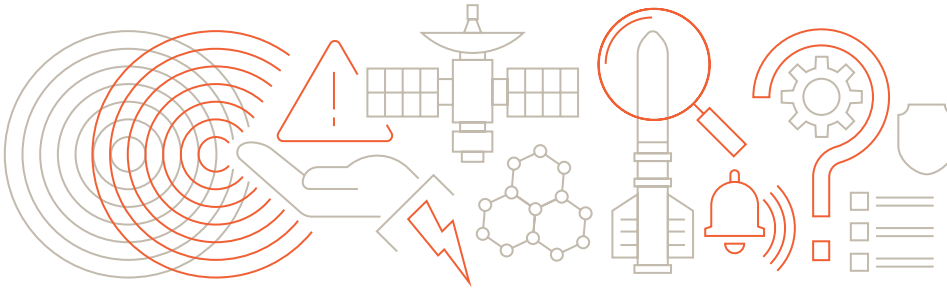
DATA AND INTELLECTUAL PROPERTY RISKS

Whether you hold sensitive medical data for genetic research or commercially sensitive information, protecting your data and intellectual property is important to you, your organisation, the public, and your partners.

Foreign states and organisations target individuals, businesses, and organisations to steal personal data, research data, commercial data, and intellectual property. This information could be used to help their own economic, military, or commercial interests.

Indigenous intellectually property including tikanga, artefacts, human materials, and cultural knowledge are particularly important to protect as they have been lost in the past to foreign researchers, pharmaceutical companies, and others.

Data and intellectual property risks should be considered alongside other risks.



KEY SECURITY CONSIDERATIONS

'Sensitive technologies' have a number of security risks. Sensitive technologies are technologies that have dual use, either now or in the future. Dual use means this technology could also have military or security applications.

Sensitive technologies are a subset of risks that need to be identified and managed through due diligence.

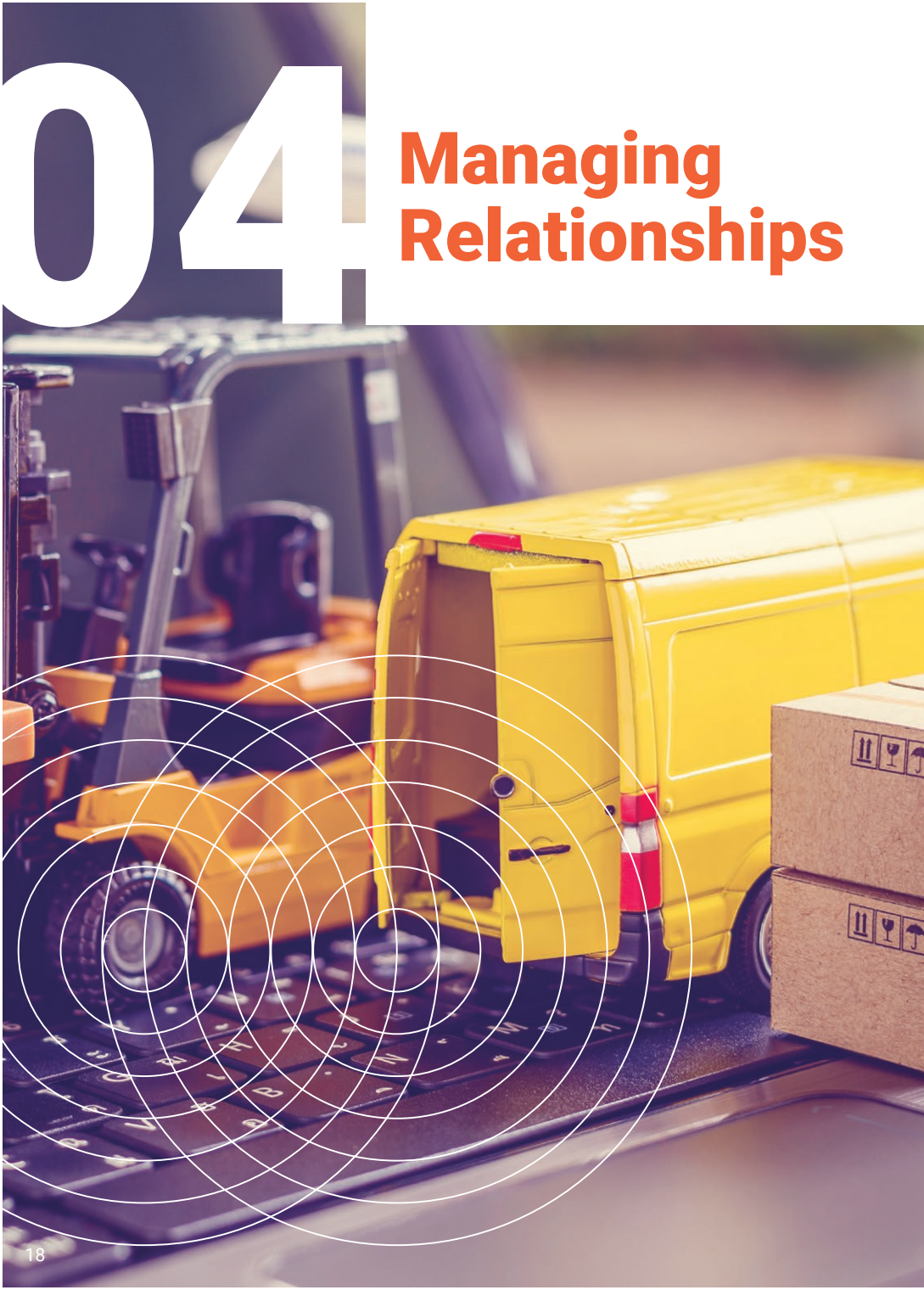
Not managing these risks could result in:

- inadvertently supporting the development of military capabilities, or the military or security apparatus of countries that do not share New Zealand's values or interests
- complicity in human rights abuses such as forced labour
- negative domestic or international reputation impacts
- loss of intellectual property.

Due diligence for sensitive or emerging technologies focuses on establishing whether the technology may have dual use applications. You can use these reference points:

- New Zealand's export control regime
- lists of sensitive technologies published by other countries
- publicly available information on the technology
- information provided by the company or research organisation itself — they often have a good idea of what the technology can be used for
- expert advice, if needed.

04 Managing Relationships



This guidance focuses on doing due diligence before entering a new business relationship with a third party, rather than managing existing relationships with third parties.

Organisations should, however, do due diligence throughout the lifecycle of a business relationship, partnership, or investment. You should respond appropriately to ensure that your current third-party relationships do not pose significant risks. This is good practice for all organisations.

To do this, start by reviewing your general portfolio of existing third parties. Use a list of key risk factors to identify those third parties that may be high-risk, and develop appropriate mitigating plans for existing contractual agreements.

Managing risks down the supply chain

You may also need to determine how far down the supply chain your due diligence efforts should go. An organisation's third party may itself use a third party to perform their contract, and so push risks further down the supply chain. You should consider the potential business and compliance risks in third-party supply chains when deciding whether to extend due diligence efforts to the suppliers of suppliers. (Good Practice Guidelines on Conducting Third-Party Due Diligence. World Economic Forum, 2013).

05 Assessing Risks

Use the following questions to help you build an approach to due diligence that is fit for your individual or organisation's purpose.

This tailored approach will help you effectively identify and assess the risks associated with proposed business relationships or research collaborations. It's part of your overall due diligence.

The degree of due diligence you do should be proportionate to the potential risks.

Your unique business and regulatory requirements will determine the specific questions you need to answer to meet your identification and assessment requirements.

WHAT DO YOU KNOW **ABOUT THE ORGANISATION?**

- What is the company name?
- What is the company structure?
- What is the shareholding structure?
- Who is the parent company?
- Who is the ultimate owner?
- What is the country of ownership?
- What background information do you have of board members, directors, key personnel, and the leadership team?
- How 'real' is the company? Is it listed on a companies' registry? Does the information match what you know of the company? What is its business history?
- Does the company, or its board members and directors, have a history of insolvency or bankruptcy, litigation, involvement in corruption or bribery, or intellectual property infringement or theft?
- Do any potential conflicts of interest exist given the company structure?

WHAT DO YOU KNOW **ABOUT NEW PARTNERS?**

- Why does a new partner want to work with you?
- What are they expecting in return for their financial support or involvement?
- Are there any current, past, or pending legal issues in any regulatory, criminal, or civil matter for the entity, its parent, subsidiaries, or key individuals?
- Does the proposed partner, or its board members and directors, have any known or suspected association with serious or organised crime groups, money-laundering groups, terrorist groups, or foreign intelligence services?
- Is the organisation associated with a country that has different strategic objectives to New Zealand, or a country with different democratic and ethical values from our own?
- Does the proposed partner have any involvement in research on behalf of the military or police with links to a hostile state?
- Could your intellectual property or research be misused or have unintended negative applications?
- Are there any legal, regulatory, or organisational policy constraints on your proposed relationship with this partner?
- Are there potential reputational or ethical risks to you or your organisation or the individuals you employ?
- Does the decision about this relationship need to be escalated within your organisation?

WHAT DO YOU KNOW **ABOUT EXISTING PARTNERS?**

- Would proceeding with the relationship raise potential conflicts of interest with existing business or research partners? Would it lead to an opportunity cost?
- Have collaborators' behaviours, interests, or external relationships changed over time into something your organisation is not comfortable with?
- Have you spoken with your existing partners about any potential conflict of interest?
- Have you considered the terms of any non-disclosure agreements? Does this include an expectation that you will need to provide visibility to existing partners?
- Will this partnership breach any existing contractual agreements that you, your department, or organisation already have?

WHAT DO YOU KNOW **ABOUT RELATIONSHIPS?**

- Are the terms of any proposed Memorandum of Understanding (MoU) or contract in keeping with the expectations of your organisation?
- Are you providing existing intellectual property (IP), research data, classified or personally identifiable data to the project or relationship? If so, how is this going to be protected?
- Who will own any new IP that is generated?
- Do you have plans for protecting resulting IP?
- What contractual requirements are you able to put in place to protect the interests of your organisation?
- What access will the partner have to your IT network? If they do have access, what visibility might this provide them to other information you manage that they should not see?
- Is there any physical separation or protection needed between business units or within research?
- How upfront and transparent is the partner about affiliations, parent partners, and their intent?
- Is a foreign entity or individual involved or influential in the arrangement, including funding?
- Are the individuals or organisations that you want to do business with free from state direction and intervention? Some governments exercise a high degree of control over universities, state-owned enterprises, and private companies.
- Are you aware of the relevant non-legal, cultural protocols for doing business with the overseas party?
- Does the overseas party belong to a jurisdiction that has a fair and equitable regime for legal remedies?
- Does the jurisdiction treat foreigners without discrimination?

HIGH-RISK FACTORS

If you identify any of these factors, your organisation should trigger its escalation processes.

- Initial searches of the internet and news services have revealed glaring problems with the third party's reputation for integrity.
- The third party or any of its senior officials have had regulatory action or legal proceedings against them because of alleged breaches of laws.
- The third party, or its parents or subsidiaries, or any of its senior officials, appear on a denied parties or persons list because of national or international sanctions, or as a result of past misconduct.
- The third party has little or no experience in the relevant industry sector or is unknown to the organisation.

References

2nd World Conference on Research Integrity. (2010, September 22). Singapore Statement on Research Integrity. Retrieved from: *www.wcrif.org/guidance/singapore-statement*

CPNI. (2020). Trusted Research Checklist: Evaluating research proposals. Retrieved from: *https://www.cpni.gov.uk/sites/default/files/engolden_checklist/Engolden-Checklist-v1.0.pdf*

Government of Canada. (2021). National Security Guidelines for Research Partnerships. Retrieved from: *https://science.gc.ca/eic/site/063.nsf/eng/h_98257.html*

National Cyber Security Centre. (2021). Supply Chain Cyber Security: In Safe Hands. Retrieved from: *www.ncsc.govt.nz/guidance/in-safe-hands/*

OECD. (2018). OECD Due Diligence Guidance For Responsible Business Conduct. Retrieved from: *http://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf*

Protective Security Requirements. (2021). Retrieved from: *https://protectivesecurity.govt.nz/*

Protective Security Requirements. (2021). Trusted Research — Guidance for Institutions & Researchers. Retrieved from: *https://www.protectivesecurity.govt.nz/assets/Campaigns/PSR-ResearchGuidancespreads-17Mar21.pdf*

Protective Security Requirements. (2020). Espionage and Foreign Interference Threats — Security advice for members of the New Zealand Parliament and Locally Elected Representatives. Retrieved from: *https://www.protectivesecurity.govt.nz/assets/Campaigns/PSR-ElectedOfficials-spreads.pdf*

World Economic Forum. (2013). Good Practice Guidelines on Conducting Third-Party Due Diligence. Retrieved from: *http://www3.weforum.org/docs/WEF_PACI_ConductingThirdPartyDueDiligence_Guidelines_2013.pdf*

For more information, go to:

www.protectivesecurity.govt.nz

psr@protectivesecurity.govt.nz

Te Kāwanatanga o Aotearoa
New Zealand Government

VERSION 1 / MARCH 2022

PSR | **Protective Security Requirements**