Managing national security risks in procurement

If you answered 'Yes' to any question in the steps of Rule 26 proceed through this guidance. You can document your application of this guidance in any way that best suits your agency.

What are national security risks and where do they arise?

National security includes the protection of sensitive New Zealand assets, both physical and digital, from threats. These include:

- espionage (for example, data theft)
- sabotage (for example, the disruption of services)
- coercion (for example, the threat of service disruption that aims to extract government concessions).

The supply of goods and services to agencies that provide, hold, or create information about public services or government policy can result in a risk to national security from foreign states.

Foreign states may target New Zealand organisations to obtain personal data, research data, and intellectual property. They may use this information to gain competitive advantage, exert their influence or exercise unwanted control.

National security risk can come up in any procurement process. But agencies should focus on procurements relating to:

- New Zealand's critical national infrastructure.
- ICT goods and services. This is due to their high value and access vulnerabilities, and the sensitive government information they can contain or process. Items include (but are not limited to) things that have internet and/or Bluetooth connectivity, phones, laptops, photocopiers, drones, facial recognition technology, surveillance equipment (including cameras), security access cards, and the IT systems and services that protect them and/or manage or store information.
- Where suppliers will have access to sensitive data about individuals.
- Business critical functions.
- Security equipment.
- Defence procurement.
- New Zealand's intellectual property and commercial interests, where New Zealand's economy would be negatively impacted if used without our permission.

When do national security risks arise in procurement

National security risks can exist at many points in the procurement lifecycle (Plan, Source, Manage) and supply chain. For example, they could relate to the supplier, parts of their supply chain or systems, changing ownership or other external pressures.

You can implement controls and mitigations at various points of the lifecycle, but they are most effective in the Plan stage.

Where to implement controls and mitigations Plan

- Ensure you understand what represents a potential national security risk with your procurement.
- If possible, design your procurement to avoid the risk. Or identify ways to manage or mitigate the national security risk.

Source

Ensure that the supplier, their systems, or their supply chains do not pose unmitigable risks. For example:

- Is the supplier actively working to challenge New Zealand's security interests, or is it effectively under the control of an entity that may wish to challenge New Zealand's security interests?
- To be able to deliver a solution, is the supplier reliant on technology from a supplier under the influence of entities working to challenge New Zealand?

Manage

Perform regular and appropriate due diligence. Keep business continuity plans are up to date, so you're ready to act if the supplier's risk profile, or ownership changes. For example, the supplier is bought by a company which is actively working to challenge New Zealand's security interests or changes the location of some of its services meaning its data holdings are now subject to new legal pressures in its home jurisdiction, or simply doesn't maintain adequate cyber security.

The level of risk posed by a supplier doesn't just depend on the nature of the supplier (or its supply chain) and needs to take into account the wider strategic threat. The risk also depends on the nature of the good or service being procured and who is procuring it. For example, a supplier may present unacceptable national security risks if engaged by the New Zealand defence sector but may not pose the same level of risk to agencies in other sectors.

For general inquiries around national security, you can ask your internal protective security advisors.

Supplier risk matrix

If you have answered 'Yes' to Questions 3a and/or 3b steps of the *Risk assessment tool for managing national security risks in procurement* (Rule 26.2), you should take additional measures to manage the risk by completing an impact and likelihood assessment for your procurement. Use the guide below.

Impact

Impact is the severity of potential outcomes if the supplier (or a supplier in its supply chain) commits an act that poses a risk to New Zealand's security.

Consider:

- What kinds of sensitive information would the supplier have access to?
- Could this information be used against individuals, or damage the agency, or New Zealand's reputation, if it was made public?
- How critical are the services being procured? What is the impact if they can be controlled by an unfriendly actor? For example, could they shut down a data centre, telecommunication network or deny access to sensitive physical premises or digital assets?
- Is the product/ service a critical component of another process/ product?
- How many people would a malicious act affect? For example, affecting 20 people is less severe than affecting hundreds or thousands.

Likelihood

Likelihood is the chance that something will happen. Consider:

- Previous performance of the supplier
- Information about the supplier's ethics, integrity, and reputation
- Whether they're pursuing legitimate commercial interests, for example, low ball offers or commercials that are well below market profitability
- Whether the supplier is owned or controlled by a foreign state

Once you have assessed the impact and likelihood, use the supplier risk matrix below to determine a risk-based approach to the procurement and identify appropriate ways to mitigate that risk.

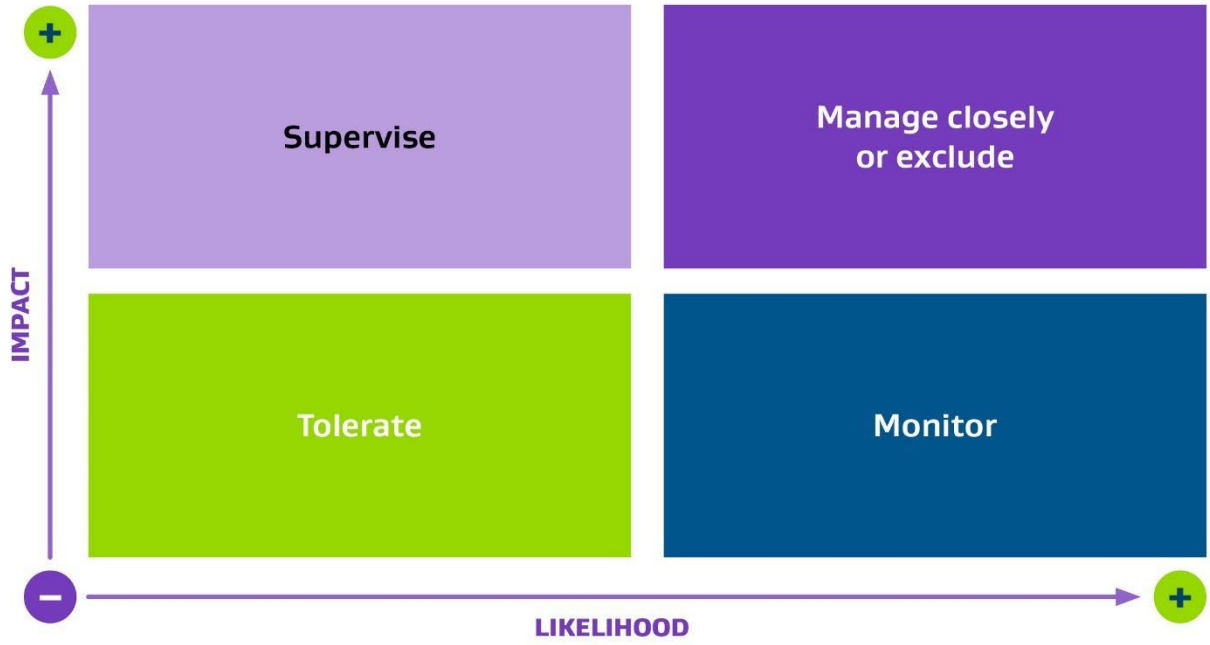
To help you manage any risk, good practice considerations and template contract clauses are provided further on.

Depending on the outcome, you should consider where this responsibility resides within the organisation (that is, "Manage Closely" or "Exclude" should sit with a more senior member like the Chief Information Officer, while "Tolerate" could sit with the Procurement Manager).

All-of-Government Contracts

All-of-Government (AoG) contracts will have the appropriate contract clauses added as the contracts are renewed, as necessary.

Figure 1: Supplier risk matrix



Tolerate

The supplier may pose some risk, but it is unlikely to be material. Use appropriate mitigations from the contract clauses and good practice considerations listed below, at your discretion.

Supervise

There could be a high impact if an incident was to occur, but the risk of an incident is low. Supervise the supplier for the length of the contract and monitor changes in its ownership and behaviour.

Consider whether to apply all the good practice considerations in Appendix 1 and if you want to use the following contract clauses in Appendix 2:

- Security and risk
- Change of control
- Audit

Monitor

There is a higher chance that an incident could occur, but the impact would be low. For example, a camera installed to monitor a conservation park is accessed by a foreign state. **Context remains key**. For instance, if the conservation park is next to a government agency's building, you would assess the risk and impact differently.

Consider if you should apply all the good practice considerations, and consider using following contract clauses:

- Conflict of interest
- Audit

- Security and risk
- Change of control

Tools for contract management – Supervise and Monitor

- You should actively manage contracts with a supplier that could pose a security risk for the lifespan of the contracts. This helps to mitigate any risk the supplier could pose. Conduct regular risk reviews
- Leverage supplier forums to resolve risk management issues shared by participants
- Develop business continuity plans and incident response plans, should an event arise.

Learn more about how to manage your contracts, including how to manage risk:

Introduction to supplier relationship management | New Zealand Government Procurement

Manage closely or Exclude

There's a high chance that an incident could occur, and the impact could be high. Monitor these contracts closely over their lifespan.

You should apply all the good practice considerations below (where possible) and should use all the contract clauses.

You may need to find another supplier if one is unwilling to agree to these terms.

Shifting from higher-risk to lower-risk suppliers could increase the cost of a contract. However, this additional cost is justified when avoiding material risks to New Zealand's democracy and economy associated with national security considerations.

If it is commercially unreasonable to switch suppliers, it's up to your agency to consider whether to proceed with the contract or not.

Given the risk likelihood and impact, you should consider excluding the supplier from the procurement under Rule 28.2i.

Excluding a supplier under the Government Procurement Rules

The Government Procurement Rules allow you to exclude a supplier on the basis that they pose a risk to national security.

Rule 28: Reasons to exclude a supplier

Rule 26 requires agencies to use the *Risk assessment tool for managing national security risks in procurement* and apply the good practices set out in this guidance when planning a procurement, to ensure that any threats to national security or the confidentiality of sensitive government information are appropriately managed.

Evidence to support your decision

Ensure you have evidence to support your decision to exclude a supplier under Rule 26. This would include:

- Documenting your security risk assessment steps of Rule 26
- Documenting your Supplier Risk Matrix.

There may be other grounds the agency could rely on, depending on what other information you gather during due diligence. For example, if you obtain classified or public information about a supplier's activities that are contrary to the high expectations set out in the Supplier Code of Conduct.

If you are considering excluding a supplier under Rule 28.2i, New Zealand's international trade obligations may also be relevant, depending on the circumstances. Discuss this with the Trade Law Unit at the Ministry of Foreign Affairs and Trade (*DM-LGL@mfat.govt.nz*).

Notifying a supplier of its exclusion

You should tell a supplier the reasons for its exclusion under Rule 28.2i, but it is not mandatory in all instances.
There may be good reasons for not providing details to the supplier, such as reliance on classified information.

Good practice considerations

RFx documents	
•	A declaration of the [Respondent]'s Beneficial Owner is included in RFx documentation. (Beneficial Owner is defined as a natural person or persons who ultimately owns or controls an interest in a company, trust or foundation. This helps to determine ownership when assessing supplier risk in Table 1, question 3(a)).
•	Include security risks as a factor for consideration in the RFx documentation's procurement assessment criteria.
•	Incorporate security risk as an area for due diligence in the assessment of responses from suppliers in all RFx documentation.
Supplier due diligence	
•	Shortlist suppliers subject to due diligence.
•	Before awarding a contract, complete due diligence on the preferred supplier(s) in relation to security risks, appropriate to the scope, risk, and value of the proposed contract.
Contract design	

•	Design the contract to include contractual controls for the level of likely security risk in the procurement and supply. Controls may include: • obligations for the supplier to notify the agency of any changes of control (for example, change of supplier), and the right for the agency to terminate upon the change of control of the supplier, without adverse contractual consequence to the agency; • reporting from the supplier on specified security-related matters; and • the right for the agency to terminate due to any change in the level or nature of the security risk, without adverse contractual consequence to the agency.
Risk monitoring and management for the life of the contract, with supporting process to maintain validity	
•	Adequately resource active monitoring of the supplier's compliance with the contract.
•	Sufficiently monitor the contract to ensure that any risks that arise are promptly managed and minimised.
•	Seek further guidance if any issue arises that could increase the security risk.

Contract clauses

These clauses provide a consistent approach across government. You can modify them to match the specific circumstances, if necessary. The intended legal protections of the clauses should not be compromised if they are modified.

You should only use these clauses when they are necessary. Complete the supplier risk matrix to identify if the procurement is likely to pose risks (that is, you answered 'Yes' to Question 1). Step 1 of the *Risk assessment tool for managing national security risks in procurement* (Rule 26.2) includes other potential mitigations that do not require contract clauses.

The contract clauses set out:

- Restrictions on changes of control of the supplier.
- Restrictions to manage any conflicts of interest.
- A right for the procurer to terminate for any change of control or conflict of interest issue, without adverse financial consequences to the procurer.
- A general audit right for the procurer, to identify any breach of the agreement or non-compliance with the Supplier's obligations under New Zealand law.
- A right for the procurer to direct the supplier to comply with security requirements before having access to the procurer's information, premises or IT systems.

Change of control

Commentary on example change of control clauses

Clause W provides the central obligation of the Supplier to notify the procurer if there is any change in the persons controlling the Supplier or any of its parent entities, or any change in the control of a subcontractor. Breach of the obligation to obtain the Agency's prior approval of the change, including at the subcontractor level, provides a right for the procurer to terminate the agreement for non-compliance of the Supplier. If the procurer exercises its termination right under this clause, then the procurer will only need to pay for the services and deliverables that have been provided by the Supplier at the date of termination.

W.1 Definitions: For the purposes of this clause W:

"**Control**" means, in relation to a person (the **first person**), where one or more persons, directly or indirectly, whether by the legal or beneficial ownership of shares, securities, partnership interests, or other equity, the possession of voting power, by contract, trust, or otherwise:

(a) has, or may have, the power to appoint or remove the majority of the members of the board of directors, or board of management, or equivalent governing body;

(b) controls or has the power, or may have the power, to control the operation of the business; or

(c) is in a position to derive more than 50% of the benefit of the existence or activities, of the first person or the ultimate or intermediate holding entity of the first person.

Reference to a "**party**", "**person**" or "**entity**" includes an individual, partnership, firm, company, body corporate, corporation, association, trust, unit trust, estate, state, government or any agency thereof, municipal or local authority and any other entity, whether incorporated or not (in each case whether or not having a separate legal personality).

W.2 Prior approval of change: The [Supplier] will not, directly or indirectly, assign, transfer or otherwise dispose of any of its rights or interests in, or any of its obligations or liability under, or in connection with, this [agreement] except with the prior consent of the [Agency] (which may be given or withheld at the [Agency]'s sole discretion). For the purposes of this clause W.2, a change of Control will be deemed to be an assignment by the [Supplier]. **W.3 Subcontracting**: The [Supplier] must:

(a) not subcontract the performance of any of the obligations of the [Supplier] under this [agreement] except with the prior consent of the

[Agency] (which may be given or withheld at its sole discretion). For the purposes of this clause W.3, a change of Control of any permitted subcontractor will be deemed to be a new subcontract by the [Supplier], which requires a further prior consent of the [Agency] under this clause W.3; and

(b) notwithstanding any permitted subcontracting, ensure:

(i) that an appropriate written agreement is in place between the [Supplier] and the subcontractor that is consistent with the terms of this [agreement] in all material respects;

(ii) that the [agreement] referred to in clause W.3(a) requires the subcontractor to seek the prior approval of the [Supplier] before any change of Control of that subcontractor; and

(iii) that it promptly notifies the [Agency] about any change of Control (or proposed change of Control) of the subcontractor.

W.4 **Termination by [Agency]**: Without limiting any other provision in this [agreement], the [Agency] may terminate this [agreement] by written notice to the [Supplier] at any time if:

(a) the [Supplier] undergoes a change of Control without the [Agency's] prior written approval;
(b) poses a potential risk to national security; or
(c) the [Supplier] breaches any of its obligations under clause W.3.

W.5 **Consequences of termination**: If this [agreement] is terminated in accordance with clause W.4:

(a) the [Agency] will only be liable to pay [Charges] that were due for the [Services and Deliverables] delivered;

(b) the [Supplier] must refund to the [Agency] all amounts paid by the [Agency], if any, for [Services and Deliverables] not delivered; and

(c) the [Agency] may recover from the [Supplier], or set off against sums due to the [Supplier], any [Charges] paid in advance for the [Services and Deliverables] not delivered, before the effective date of termination.

Conflict of interest

Commentary on example conflicts of interest clause

Clause X provides a general obligation for the Supplier to notify the procurer of any conflict of interest that may arise before the commencement, or during the term, of the agreement. The procurer can instruct the Supplier on how the conflict must be managed. If the procurer considers any conflict cannot be managed, the procurer has a right to terminate the agreement and from the date of termination, the procurer will only need to pay for the services and deliverables that have been delivered by the effective termination date.

X.1 **Definitions:** For the purposes of this clause X:

"**Conflict of Interest**" means any matter, circumstance, interest or activity of the [Supplier], its [Personnel] or [subcontractors], arising by whatever means that directly or indirectly conflicts with:

(a) the obligations of the [Supplier] to the [Agency] under this [agreement]; or

(b) the interests of the [Agency] in relation to this [agreement], or otherwise impairs or might appear to impair the ability of the [Supplier] (or any of its [Personnel] or [subcontractors]) to provide the [Services and Deliverables] to the [Agency] under this [agreement], diligently, independently, impartially and in the best interests of the [Agency].

X.2 **Inquiry**: The [Supplier] must:

(a) during the term of this [agreement], make diligent inquiry whether it has any actual, potential or perceived Conflicts of Interest;

(b) if there is any actual, potential or perceived Conflict of Interest, promptly notify the
[Agency] of the relevant details of such Conflict of Interest; and

(c) take all actions reasonably required by the [Agency] to resolve, manage or remove any such Conflict of Interest; and

(d) unless otherwise agreed by the [Agency] in writing, immediately suspend the provision of the [Services and Deliverables] until such time as the [Agency] is satisfied that such Conflict of Interest has been resolved, managed or removed.

X.3 **Termination**: If the [Agency] considers the [Supplier] has an actual Conflict of Interest of sufficient gravity that the [Supplier] can no longer provide the [Services and Deliverables] for it, the [Agency] may, by written notice to the [Supplier], terminate this [agreement] with immediate effect on the date of termination specified in that notice.

X.4 **Consequences of termination**: If this [agreement] is terminated in accordance with clause X.3:

(a) the [Agency] will only be liable to pay [Charges] that were due for the [Services and Deliverables] delivered;

(b) the [Supplier] must refund to the [Agency] all amounts paid by the [Agency], if any, for [Services and Deliverables] not delivered; and

(c) the [Agency] may recover from the [Supplier], or set off against sums due to the [Supplier], any [Charges] paid in advance for the [Services and Deliverables] not delivered, before the effective date of termination.

Audit

Commentary on example audit clause

Clause Y provides the procurer with a general audit right to review any breach of the agreement or law (which will include any breach of the Supplier's obligations regarding security, conflicts of interest and change of control).

Y.1 **Audit**: Without limiting any other right for the [Agency] to audit the [Supplier] under this [agreement], the [Supplier] will, on reasonable prior written notice from the [Agency], give the [Agency] (and the [Agency's] personnel, internal and external auditors, and advisers) ("**Audit Personnel**") full access, during normal business hours, to:

(a) all premises at which or from the [Supplier] performs its [agreement];

(b) any [Supplier] personnel (including any [subcontractors]); and

(c) any information, data, accounts, documents and records to the extent relating to the performance of this [agreement], operated or held by or on behalf of the [Supplier] and its [subcontractors],

to the extent necessary to enable the [Agency] (and the other Audit Personnel) to:

(d) audit the [Supplier's] compliance with this [agreement]; and/or (e)

comply with any applicable laws.

Y.2 **Assistance**: The [Supplier] will, and will ensure its personnel and [subcontractors], assist the [Agency] (and/or the other Audit Personnel) in a timely manner with any audit conducted under this clause Y, including by making their relevant premises, personnel, systems, information, data, accounts, documents and records available to the [Agency] (and the other Audit Personnel).

Y.3 **Costs**: The [Agency] will meet the costs of any audit unless the audit discloses a breach of this [agreement] or law. In that case, the [Supplier] will meet the [Agency's] audit costs.

Y.4 **Non-compliance**: Without limiting any of the [Agency's] other rights or remedies, if any audit is conducted under this clause Y discloses any failure to comply with this [agreement] by the [Supplier], the [Supplier] will promptly remedy the non-compliance. [The [Supplier] will refund any amounts overcharged by the [Supplier] within [5] days of completion of an audit and delivery of an audit report.]

Security and risk

Commentary on example security and risk clause

Clause Z provides that if the supplier requires access to the procurer's information, premises or IT systems in order to provide the services and deliverables, the supplier, their personnel and the supplier's subcontractors must comply with any security requirements specified by the procurer. This will include complying with any relevant security checks and clearances required by the procurer.

The procurer should ensure that it clearly communicates its security requirements (including security policies and procedures) to the supplier as part of the procurement process and during the term of the agreement.

The supplier must also notify the procurer if the supplier has any change of circumstances that may affect their capacity to provide the services and deliverables in accordance with the procurer's security requirements or if any material that the procurer has provided to the supplier has been lost or disclosed to unauthorised persons.

Z.1 Definitions: For the purposes of this clause Z:

"[**Agency] Operating Environment**" means all aspects of the [Agency's] information technology and telecommunications environment, including hardware, operating systems, middleware, network systems, applications, processing facilities, support systems and desktops, whether in a production or other environment from time to time.

"[**Agency] Site**" means the premises and other property sites specified by the [Agency] from time to time at or from which the [Supplier] will provide the [Services or Deliverables]. **Z.2 General security requirements**:

(a) If the [Supplier] requires access to any [Agency] Site, the [Agency] Operating Environment, or any [Agency] information, from time to time to provide the [Services and Deliverables], the [Supplier] will:

(i) comply with all security requirements notified to the [Supplier] by the [Agency] from time to time; and

(ii) ensure that its [Personnel] and [subcontractors] are aware of and comply with those security requirements.

(b) The [Supplier] will:

(i) ensure that its [Personnel] undertake and satisfy the requirements of all security checks and clearances required by the [Agency]; and

(ii) notify the [Agency] of any changes to circumstances that may affect the [Supplier's] capacity to provide the [Services and Deliverables] in accordance with the security requirements contained in this [agreement] and such requirements notified to the [Supplier] from time to time.

(c) The [Supplier] must promptly report to the [Agency] any instance in which it is known or suspected that material (in any format and including information) furnished or generated pursuant to this [agreement] has been lost, or disclosed to, or accessed by, unauthorised persons.

.The [Supplier] must not cause the [Agency] to breach any mandatory requirement in any tier of the Protective Security Requirements available at https://protectivesecurity.govt.nz/.