New Zealand Government
Te Kāwanatanga o Aotearoa

Corruption prevention guide

Managing corruption risk in the New Zealand public sector

SFO
SERIOUS FRAUD OFFICE
TE TARI HARA TĀWARE

Counter Fraud Centre
TAUĀRAI HARA TĀWARE

The Serious Fraud Office Te Tari Hara Tāware is the lead law enforcement agency for investigating and prosecuting serious or complex fraud, including bribery and corruption. It works to strengthen the public sector's resilience to fraud and corruption through its Counter Fraud Centre Tauārai Hara Tāware.

June 2026

Serious Fraud Office Te Tari Hara Tāware
Counter Fraud Centre Tauārai Hara Tāware

PO Box 7124
Victoria Street West
Auckland 1141
Aotearoa New Zealand

Phone 0800 109 800
Email counterfraud@sfo.govt.nz
Web sfo.govt.nz/counter-fraud/counter-fraud-centre

New Zealand Government
Te Kāwanatanga o Aotearoa

Contents

1

Introduction

Aotearoa New Zealand has a strong reputation for integrity and open and transparent government. Public service values are well established and most public sector employees act with honesty and professionalism every day.[1]

But no country is free from corruption risks. Corruption does not need to be widespread to cause harm. A single incident can damage public confidence, weaken trust in government institutions and affect New Zealand's international reputation as a safe place to do business.

This guide is for all public sector employees. It explains what corruption is, outlines common corruption risks in plain language, highlights the areas (also referred to as domains) where those risks are most likely to arise, and offers practical steps to help protect your organisation, your colleagues and the communities we serve.

Agencies should assess their own risk profile and take steps that are proportionate and appropriate to their size and complexity. Agencies should also make sure to comply with the relevant laws and guidelines for functions (e.g. employment, procurement, finances) at all times. Organisations that operate internationally may face higher exposure and should also consider relevant international standards and local regulatory requirements.

Working with integrity is a shared responsibility. Together, we can maintain a public sector that is trusted, fair, accountable and focused on delivering the best outcomes for New Zealanders.

[1] See https://www.publicservice.govt.nz/guidance/standards-of-integrity-and-conduct.

The corruption problem

Corruption is often hidden. It involves secrecy, deception and deliberate efforts to avoid detection, which means reliable data is limited. Perception surveys can tell us how people feel about corruption, but they cannot fully show how often it occurs or what it looks like in practice.

Like other countries, New Zealand faces challenges in understanding the true scale of corruption. It is estimated that in New Zealand anywhere between $601 million and $12.97 billion taxpayer dollars are lost every year to fraud and error, including corruption.[2]

New Zealand consistently ranks highly in the Transparency International Corruption Perceptions Index,[3] reflecting our strong integrity settings and public service values. However, while some countries have reduced their perceived levels of corruption and improved their ranking, New Zealand's ranking has dropped every year since 2021. Corruption remains a serious threat. It takes hold when vigilance declines or controls weaken.

How corruption undermines economic growth and social cohesion

Corruption diverts public resources, distorts decision making, undermines trust in institutions and weakens outcomes across economic, social and regulatory systems. It compromises fairness, reduces the quality and safety of services, and damages New Zealand's reputation as a reliable and transparent place to do business.

Institutional and democratic impacts

When integrity standards are not upheld, confidence in public institutions declines. Trust in procurement processes, funding decisions and regulatory enforcement is weakened. Decisions influenced by corruption serve private interests rather than the public good, which undermines fairness, accountability and the legitimacy of government. This erosion of trust can reduce civic participation and confidence in democratic processes.

---

[2] Government Counter Fraud Function, 2021.

[3] See https://www.transparency.org/en/cpi.

Economic impacts

Corruption increases costs, distorts markets and discourages fair competition and investment. Businesses that rely on merit are disadvantaged when contracts or opportunities are influenced by improper relationships or payments. Public funds are used inefficiently, resulting in poorer services and reduced value for taxpayers. Over time, this weakens economic productivity and growth.

Social impacts

Corruption contributes to inequality by directing resources and opportunities away from those with the greatest need or merit. It can reduce access to quality services and erode public confidence in fairness and equal treatment. This weakens social cohesion and trust between communities and institutions.

Security and law enforcement risks

Corruption within public roles can undermine enforcement systems and create vulnerabilities that may be exploited by organised crime. Misuse of authority or access to information can compromise regulatory, border or law enforcement functions, reducing the effectiveness of safeguards designed to protect the public.

Environmental impacts

Corruption can result in inadequate enforcement of environmental protections, leading to pollution, resource depletion and long-term damage to ecosystems. These impacts threaten our natural resources, key industries such as tourism and agriculture, our cultural values and the wellbeing of current and future generations.

Individual consequences

Individuals involved in corruption face serious legal and personal consequences, including criminal conviction, fines, imprisonment, loss of employment and long-term reputational damage.

Examples of serious corruption in New Zealand

- **Roading contract kickback scheme:** Five people were convicted in a roading maintenance corruption case. One subcontractor alone paid $626,000 in kickbacks and gifts to a former manager to secure contracts.[4]
- **IT contractor kickbacks:** Two former contractors involved in an IT upgrade for Spark New Zealand were sentenced to three years' imprisonment for a $4.1 million kickback scheme. Over $20 million in contracts was received by the defendant on the recommendation of the second defendant, without disclosing the relationship.[5]
- **Procurement bribery in health:** A former senior health employee accepted over $250,000 from medical equipment and software supply companies in exchange for assisting the companies to secure district health board business.[6]
- **Immigration bribery:** A business owner was sentenced to four years' imprisonment for unlawfully employing a foreign national in New Zealand and assisting others to breach their visa conditions. The individual bribed an Immigration New Zealand official to secure visas and favourable treatment, enabling the unlawful recruitment of foreign nationals who were subsequently exploited while working illegally in New Zealand.[7]
- **Airport insider corruption enabling drug importation:** An Air New Zealand baggage handler was jailed for his role in a methamphetamine importation syndicate, facilitating the smuggling of more than 110 kilograms of methamphetamine using his position to bypass customs checks.[8]

[4] See https://www.sfo.govt.nz/media-cases/cases/auckland-road-maintenance-case.

[5] See https://www.sfo.govt.nz/media-cases/media-releases/it-contractor-pleads-guilty-to-paying-4-1-million-in-kickbacks.

[6] See https://www.sfo.govt.nz/media-cases/media-releases/guilty-pleas-in-sfo-corruption-case-involving-supply-of-medical-equipment.

[7] See https://www.immigration.govt.nz/about-us/news-centre/samoan-national-sentenced-for-migrant-exploitation-and-other-charges.

[8] See https://www.stuff.co.nz/nz-news/360547396/air-new-zealand-baggage-handler-jailed-part-meth-importing-syndicate.

2

Understanding corruption

Corruption is the abuse of entrusted power for private gain. In the public sector, it means using your role to benefit yourself or others, including your family, friends or any business you are connected to.

Corruption does not always involve large sums of money. It can begin with small decisions that compromise fairness, trust and impartiality, and can occur in any organisation at any level. It involves the deliberate abuse of entrusted power. People may not start out intending to be corrupt – there can be a gradual progression from poor judgement to intentional misconduct.

Why corruption happens

Corruption and fraud rarely happen by accident. The fraud triangle is a useful framework for understanding the conditions that can lead to fraudulent or corrupt behaviour. When these factors intersect, the risk of fraud or corruption increases:[9]

- **Pressure:** the motivation for people to commit fraud. These pressures might be personal, financial or work-related.
- **Opportunity:** a gap or weakness in a system that can be exploited.
- **Rationalisation:** when a person justifies their fraudulent behaviour, convincing themselves it is acceptable or deserved.

[9] Find out more about the fraud triangle: https://www.sfo.govt.nz/counter-fraud/guidance/fraud-101.

How people are drawn into corruption

Not everyone who becomes involved in corruption sets out to do something wrong. Some people are coerced, compromised or gradually drawn by others into behaviour they would not otherwise consider.

Skilled manipulators can appear friendly, generous or professionally helpful. Even experienced employees may not realise what is happening until they are already compromised, at which point self-reporting is rare. Manipulation can come from outside the organisation or from colleagues and managers, and collusion between internal and external actors can appear procedurally correct, making it hard to detect.

Common manipulation tactics include:

- **Coercion:** using threats or pressure to force someone to act improperly. This may include threatening to expose personal information, pressure from powerful individuals or warnings that refusal will harm a person's role, reputation, safety or the safety of someone close to them. For example, an employee is threatened with violence unless they approve a fraudulent payment.
- **Compromise:** exploiting personal vulnerabilities or prior misconduct to create leverage over someone. This can include financial stress, addiction, relationship difficulties, or accepting gifts or hospitality in breach of policy. For example, an employee accepts a small improper gift, then feels unable to refuse larger favours. Once someone has taken even a minor improper step, they may feel unable to stop.
- **Grooming:** a deliberate, staged process of building a relationship over time to make improper requests feel normal or justified. Techniques include small gifts, flattery, personal rapport, minor favours that gradually escalate, and encouraging communication outside official channels. For example, a supplier builds trust through informal contact and minor favours before gradually requesting policy breaches that no longer feel unusual.

Awareness is a key control. Recognising these manipulative tactics early is one of the most effective ways to avoid being drawn into corrupt behaviour.

Who is involved

Corruption can involve people in many different roles, both inside and outside an organisation. A person's role often shapes how corruption occurs, how it is concealed and how difficult it is to detect. The following are common types of corrupt actors and the risks they present.

- **Internal actors** are people inside an organisation who misuse the trust or authority that their role provides. This is known as an insider threat. It can involve any role – such as employees, managers, contractors or senior leaders – and typically involves using knowledge of systems or processes for personal benefit or to benefit someone known to them.[10]
- **External actors** are individuals or groups outside an organisation who seek to influence public sector employees or exploit weaknesses within processes. They may use gifts, hospitality, personal relationships, improper political pressure or informal networks to gain an unfair advantage. Common examples include suppliers seeking favourable contract terms, consultants or lobbyists misusing access to influence decisions, grant recipients pressuring assessors, organised crime groups targeting border or regulatory systems, or members of the public seeking to avoid penalties or bypass eligibility requirements.
- **Collaborative or networked actors** involve internal and external parties working together. This form of corruption is among the hardest to detect because corrupt actions can appear to follow normal business processes. Examples include an employee sharing confidential tender information with a preferred supplier, a contractor inflating invoices with the cooperation of internal employees, or employees using their position to benefit family members or close associates.
- **Professional enablers** are people in trusted and regulated professions, such as lawyers, accountants, bankers, real estate agents and consultants, whose specialist skills can support corrupt activity even when they do not directly benefit. They may move or conceal funds, establish shell companies or certify misleading documents. Enabling corruption is not always intentional. Failing to apply appropriate professional scepticism, ignoring warning signs or choosing not to ask questions can still contribute to corrupt conduct.

Identifying who may be involved and how they operate is critical to understanding corruption risk and strengthening controls across people, processes and systems.

[10] Find out more about insider threat: https://www.sfo.govt.nz/counter-fraud/guidance/insider-threat.

3

Common forms of corruption

Corruption is a group of behaviours that share one core feature: the misuse of entrusted power for private gain.

Recognising how corruption appears in day-to-day work is essential, as some forms are obvious, while others are subtle, and many escalate over time. For example, an individual may fail to declare a conflict of interest, then go on to provide confidential information to a supplier during the procurement process, accept a bribe to influence the award of a contract, and later enter into an ongoing arrangement where they receive payments in return for continuing to direct business to that supplier.

The following behaviours are some of the more common ways in which corrupt intentions can be achieved. Often more than one behaviour is displayed at once.

Abuse of power and influence peddling

This occurs when someone uses their position, authority or access to decision makers to obtain an improper advantage for themselves or others. It can arise wherever discretionary power exists, not only among senior leaders.

Forms of abuse of power and influence peddling include:

- **Extortion:** demanding money, favours or compliance through threats, including threats to withhold a service or take adverse action.
- **Electoral manipulation:** using public resources, pressure or incentives to influence election outcomes, including vote buying or blocking participation.
- **Influence peddling:** claiming the ability to influence official decisions in exchange for money or benefits, whether or not the claim is genuine.

Example

A procurement employee suggests to a contractor that their bid might not succeed without a payment being made to smooth the process. No overt demand is made; the pressure comes through hints and knowledge of the employee's discretionary power.

Improper benefits

This form of corruption involves offering, seeking or accepting something of value to influence a decision, action or inaction. Benefits can be financial or non-financial and may be provided before as an incentive or afterwards as a reward. In all cases, they undermine fair and impartial decision making.

Forms of improper benefits include:

- **Bribery:** offering or accepting an inducement or reward to influence official action or inaction. Bribes can take many forms, including money, employment, hospitality or gifts, and can be offered directly or indirectly to the person being bribed.
- **Kickbacks:** concealed payments or rewards given to someone who approved or facilitated a contract, which may be disguised through inflated invoices or complex subcontracting arrangements.
- **Unlawful campaign contributions:** providing money to political campaigns or parties in return for favourable policy, regulatory treatment or contract opportunities.

Example

A contractor made undisclosed payments and provided travel and hospitality to a public sector manager. In return, the manager supported the contractor to secure work and contracts, undermining fair procurement processes.

Exploited or undisclosed conflicts of interest

A conflict of interest arises when a person's private interests overlap with their public duties in a way that could affect, or be perceived to affect, their judgement. Not all conflicts result in corruption. Conflicts of interest become a corruption risk when they are not declared or appropriately managed, allowing private interest to influence, or appear to influence, official duties.

Forms of exploited or undisclosed conflicts of interest leading to corruption include:

- **Self dealing:** a public official making decisions in an official capacity that benefit personal financial interests.
- **Misuse of official information:** using non-public or confidential official information for personal benefit.
- **Biased decision making:** allowing personal relationships or expected benefits to influence decisions.

Example

A staff member involved in a procurement fails to disclose that a close associate owns one of the bidding companies. During the process, they share confidential information held by their agency about competitors' bids and influence the evaluation in that company's favour. The company is awarded the contract.

Misuse of resources

This form of corruption involves the theft, diversion or improper use of public assets, funds or organisational processes for private benefit. It can begin with minor boundary-pushing behaviours that become normalised and escalate over time.

Forms of misuse of resources include:

- **Theft:** taking money or assets that an employee is responsible for managing or safeguarding.
- **Ghost workers and payroll fraud:** paying salaries to people who do not exist or keeping former employees on payroll systems.

- **Procurement fraud:** approving payment for goods or services not delivered, inflating contract values or splitting contracts to avoid approval thresholds.
- **Misuse of public assets:** using government vehicles, equipment, premises or employees for private purposes.

Example

A manager approves invoices from a supplier that no longer operates. Over several years, hundreds of thousands of dollars are paid into a bank account controlled by the manager's family member. Weak verification controls in a high volume payment system allows the scheme to continue undetected.

Fraud and deception

Fraud involves a deliberate deception to obtain something a person is not entitled to, such as using false documents, manipulated records or making misleading statements. Acts of fraud perpetrated with the intention of abusing power for personal gain may also be corrupt.

Forms of fraud and deception include:

- **Financial reporting fraud:** falsifying accounts, performance data or compliance records to misrepresent an organisation's financial health or conduct.
- **Invoice and billing fraud:** submitting false or inflated invoices or billing for work that was not completed.
- **Forgery and falsification:** creating or altering official documents, licences or records to obtain a benefit or avoid scrutiny.
- **Procurement manipulation:** rigging tender evaluations, altering assessment records or leaking bid information to favour a predetermined supplier.
- **Subsidy and grant fraud:** providing false or misleading information to obtain public funds or benefits.

Example

A contractor files certified reports claiming that major infrastructure works have been completed. An audit later finds that much of the work never occurred. The false reports were supported by fabricated inspection records signed off by a site supervisor with a financial interest in the contractor.

Misuse of information

Public sector roles often involve access to sensitive or non-public information, which creates opportunities for corruption if that information is wrongfully disclosed or misused. This behaviour can be difficult to detect and highly damaging.

Forms of misuse of information include:

- **Improper use for personal gain:** using non public information obtained through one's role to make personal financial decisions.
- **Leaking information for personal gain:** disclosing restricted government information in exchange for money or favours.
- **Data manipulation:** altering statistics, audit findings, assessments or performance data to conceal poor performance or support a corrupt outcome.
- **Unauthorised access and insider threat:** misusing system access to retrieve, delete or alter information without a legitimate purpose.
- **Surveillance and intelligence abuse:** misusing law enforcement or intelligence systems for personal, political or commercial purposes rather than authorised public duties.

Example

An employee learns of a rezoning decision before it is publicly announced and shares this information with a developer they know. The developer purchases the land at a lower, pre-zoning price. Once the rezoning is announced the land increases in value and is sold for a significant profit. The employee later joins the developer's company, raising concerns about a conflict of interest and misuse of insider information.

Collusion and market manipulation

Collusion occurs when people or organisations secretly coordinate to fix outcomes or avoid competition. In procurement, it undermines competitive tendering and inflates costs to government. In regulatory and political settings, it can distort markets and democratic processes.

Forms of collusion and market manipulation include:

- **Bid rigging:** competitors secretly agreeing in advance who will win a contract.

- **Price fixing:** competitors agreeing to set prices above competitive levels.
- **Market division:** competitors agreeing to allocate markets by geography, customer type or contract.
- **Electoral collusion:** coordinating activities to predetermine electoral outcomes or suppress opposition.

Example

Three firms competing for regional maintenance contracts secretly coordinate their bidding over a six-year period. They take turns being the "winning" bidder, while the other firms submit cover bids that are deliberately overpriced or non-compliant tenders, designed to make the chosen bid appear competitive. As a result, contract prices remain consistently higher than market benchmarks and genuine competition is excluded.

Concealment of proceeds of crime

Concealing the proceeds of crime involves hiding or disguising money or benefits gained from wrongdoing to make them appear legitimate. This hides the original misconduct, protects corrupt actors and reduces the risk of detection. These behaviours follow various forms of corruption but also act as powerful enablers of ongoing misconduct.

Forms of concealment of proceeds of crime include:

- **Money laundering:** disguising the origin of illegally obtained funds.
- **Use of shell companies or obscuring beneficial ownership:** hiding who owns or controls assets or entities to create distance and avoid scrutiny.
- **Asset acquisition:** hiding stolen wealth in property, luxury goods or digital assets.
- **Falsified records:** creating or altering records to obstruct oversight.

Example

Over several years, an employee dishonestly takes funds they are responsible for and channels the money through shell companies before investing in property held under a nominee's name.

Affiliation and patronage practices

These practices sustain corruption over time through networks of reciprocal benefit, informal obligations and loyalty, resulting in outcomes that are influenced by personal relationships over merit, fairness or public interest. Rather than involving a single improper exchange, these practices create sustained advantages and enduring influence that erode impartial decision making.

Forms of affiliation and patronage practices include:

- **Public-private role transitions (revolving door):** movement between public sector roles and private entities that creates an improper advantage.
- **Nepotism:** favouring family members in hiring or access to opportunities.
- **Cronyism:** favouring friends or associates regardless of merit.
- **Clientelism:** distributing jobs, contracts or resources in exchange for loyalty or political support.

Example

A former senior public official joins the board of a company that later wins several government contracts managed by the official's former subordinates. Each decision appears defensible in isolation, but the pattern raises concerns about improper influence and compromised impartiality.

How these risks link together

These forms of corruption are not separate. In practice, corruption often involves multiple, overlapping behaviours. Bribery can lead to procurement fraud. Procurement fraud can generate proceeds that must be concealed through money laundering. Concealment may rely on insider access, misuse of information or falsified records. Over time, patronage networks may emerge that protect, reward or normalise this behaviour.

For public sector employees, this has a practical implication: when you notice one warning sign, consider whether related risks may also be present. Misuse of information may signal an undeclared conflict of interest. Repeated awards to the same supplier may suggest collusion or kickbacks. Unexplained wealth may point to bribery, fraud or dishonest misuse of public funds.

4

Where corruption is most likely to occur

Corruption can occur in any organisation and at any level. However, certain key operational areas carry higher risk because they involve greater discretion, higher financial value, external influence or access to sensitive information. Understanding the domains where these risks are concentrated allows agencies to strengthen controls, target prevention efforts and help employees recognise vulnerabilities in their everyday work.

Procurement and contract management

Procurement and contract management are consistently assessed as among the highest-risk functions in the public sector for fraud and corruption. High-value spending, competitive tendering processes and close supplier engagement create inherent vulnerabilities to undue influence, process manipulation and misuse of public funds. These vulnerabilities are particularly acute where discretionary decisions and supplier relationships can be leveraged to favour certain outcomes or conceal improper conduct.

Why the risk is higher

- High financial values associated with purchasing and contract decisions.
- Significant discretion in supplier selection, evaluation scoring, negotiations and contract management.
- Frequent interaction with suppliers seeking commercial advantage.

- Complex, multistage processes that can be bypassed, altered or poorly documented.
- Time pressures that may encourage shortcuts and reduce the level of scrutiny applied.

Red flags and controls

Table 4.1: Potential procurement and contract management red flags and possible controls

Potential red flags	Possible controls
Specifications that favour one supplier	
▸ Requirements are unusually narrow or overly specific. ▸ Product descriptions closely match a single brand or supplier offering. ▸ A supplier appears "ready" or pre-positioned before the tender is released.	▸ Obtain an independent review of specifications by procurement or a suitably qualified third party. ▸ Involve the procurement team to test for market fairness and supplier neutrality. ▸ Clearly document how the requirements were developed and the rationale for key decisions.
Inflated, late or suspicious contract variations	
▸ Costs increase unexpectedly or disproportionately. ▸ Scope changes occur without clear rationale or documented justification. ▸ Variations repeatedly benefit the same supplier.	▸ Require complete supporting documentation and clear business case for each variation. ▸ Refer variations to finance or procurement for independent review and approval. ▸ Pause or withhold approval until appropriate scrutiny and assurance is completed.

Potential red flags	Possible controls
Invoices that do not match deliverables	
▸ Work has not yet been completed or verified. ▸ Duplicate, repeat or otherwise unexplained invoices are submitted. ▸ Invoice descriptions are vague or generic (e.g. "general services", "support fees", "management fees").	▸ Verify delivery and completion with the project manager or technical lead. ▸ Request itemised invoices and evidence of work performed. ▸ Withold or decline payment until the invoice is fully validated.

Recruitment, appointments and payroll

Recruitment and appointments are a high-risk domain for corruption because they determine who gains access to public resources, decision making authority and long-term career opportunities. Where recruitment processes are influenced by personal relationships, undeclared conflicts of interest or the misuse of confidential information, both the integrity and capability of the public sector are undermined.

Payroll processes can be exploited where employees with access to human resources or payroll systems create fictitious employees, keep former employees' records active, or manipulate pay rates, allowances or bank account details without authorisation.

Corruption risks arise where managers or employees knowingly falsify records, collude to approve improper payments or use payroll processes to reward loyalty, secure favour or avoid scrutiny. These risks are elevated where human resources and payroll functions are controlled by the same person or small team, and where payroll records are accepted on face value without independent verification.

Why the risk is higher

- Panel discretion in interpreting criteria, weighting experience and ranking candidates.
- Potential for senior level influence over shortlisting or final selection decisions.
- Access to confidential candidate information and referee reports.
- Social or personal relationships between candidates and employees involved in the process.
- Pressure to "get someone in quickly," increasing the likelihood of shortcuts or inadequate documentation.
- Weak separation of duties between human resources, payroll processing and financial approvals.
- Payroll records accepted on face value without independent verification.
- High transaction volumes that can make individual anomalies harder to detect.
- Limited audit of system changes, including pay rate adjustments, bank account updates and employee status changes.
- Opportunities for collusion between employees and supervisors to facilitate improper payments.

Red flags and controls

Table 4.2: Potential recruitment, appointment and payroll red flags and possible controls

Potential red flags	Possible controls
Undeclared conflicts of interest on the panel	
▶ A previously undisclosed personal or professional relationship with a candidate is identified during or after the recruitment process. ▶ Information emerges that a panel member participated in assessment or scoring despite a relationship that should reasonably have been disclosed. ▶ An employee strongly advocates for a particular candidate without reference to merit or evidence.	▶ Require all panel members to formally declare conflicts of interest before shortlisting and interviews. ▶ Remove conflicted panel members from shortlisting, scoring or decision making where the conflict cannot be effectively managed. ▶ Ensure all recruitment decisions are documented, evidence-based and aligned to the selection criteria.
Inconsistent or unjustified scoring	
▶ A candidate is shortlisted or appointed despite not meeting mandatory criteria. ▶ Significant variation in panel scores without clear explanation. ▶ Interview notes or assessment records do not support the final ranking decision.	▶ Require each panel member to document written scoring rationales against the agreed criteria. ▶ Complete scoring independently before panel discussion to reduce group influence. ▶ Escalate concerns about potential undue influence or irregular scoring to human resources.

Potential red flags	Possible controls
Senior-level pressure to select a preferred candidate	
▶ A manager signals who "should get the role" outside the formal process. ▶ Attempts are made to override panel scores and rankings. ▶ Use of phrases such as "they're the right fit" without merit-based justification.	▶ Reinforce the principle of merit-based selection and documented decision making. ▶ Record all panel decisions, discussions and reasons for final selections. ▶ Escalate suspected undue influence to human resources or integrity teams.
Unauthorised or fraudulent payroll changes	
▶ Pay rates, allowances or classifications are changed without proper approval or audit trail. ▶ Payments continue to be made to former or inactive employees with management knowledge. ▶ Duplicate employee or bank records are maintained without clear explanation.	▶ Maintain clear separation of duties across human resources, payroll and approving managers. ▶ Conduct regular exception-based payroll reviews focusing on management overrides and changes. ▶ Promptly disable system access and payroll records when employee status changes.

Secondary employment

Secondary employment (also called outside employment or additional work) creates a corruption risk where private interests intersect with official duties, increasing the likelihood of misuse of public assets, compromised impartiality and conflicts of interest.

Even occasional or unpaid work can give rise to real or perceived conflicts of interest if it is not properly declared and appropriately managed.

Why the risk is higher

- Actual or perceived conflicts of interest when outside work relates to an employee's official responsibilities.
- Competing loyalties between public duties and private business or commercial interests.
- Use of public time, information or resources to support private work.
- Reduced independence if outside clients, employers or business interest are affected by organisation decisions.
- Increased opportunity for misuse of confidential information for private commercial advantage.

Red flags and controls

Table 4.3: Potential secondary employment red flags and possible controls

Potential red flags	Possible controls
Undeclared secondary employment	
▶ Information emerges that an employee is operating a private business or undertaking paid outside work that has not been declared. ▶ Outside work is identified through social media, customer complaints or third-party information. ▶ An employee is unable to clearly explain how they separate secondary employment from their public role.	▶ Require the employee to formally declare secondary employment and business interests. ▶ Assess whether the secondary employment creates a real, potential or perceived conflict of interest. ▶ Escalate to human resources or integrity teams for review, decision making and ongoing monitoring.
Outside work overlapping with official duties	
▶ An employee's secondary employment is in the same sector or industry they regulate, oversee or influence. ▶ Private clients may benefit from the employee's public role. ▶ Knowledge, insights or relationships from an employee's public sector role appear to be used to support private work.	▶ Conduct a documented conflict of interest assessment. ▶ Restrict or decline the secondary employment where conflicts cannot be effectively managed. ▶ Implement appropriate mitigations in place (e.g. removal from certain functions or decisions).

Potential red flags	Possible controls
Use of organisation time, resources or systems for private work	
▸ Use of work hours to send invoices, emails or documents related to their private business activities. ▸ Use of organisation IT systems, vehicles or contacts for private gain. ▸ Blurred boundaries between public and private work activities.	▸ Reinforce acceptable use policies and expected standards of conduct. ▸ Review system access and monitor usage where risk indicators are present. ▸ Escalate for investigation where misuse is deliberate, repeated or involves sensitive information.

Financial delegations and asset management

Financial delegations and asset management functions present corruption risks where employees misuse delegated authority over public money or assets for private gain. Where oversight is limited or controls rely on individual judgement, corrupt practices may become normalised and difficult to detect.

Why the risk is higher

- Delegated authority to approve expenditure or payments with limited independent oversight.
- Direct access to financial systems, purchasing cards or asset registers.
- High volumes of routine transactions that draw less scrutiny.
- Ability to conceal improper payments through coding, journal entries or asset movements.
- Opportunity for unauthorised private use of vehicles, equipment or property.
- Weak segregation of duties, particularly in smaller teams or regional locations.

Red flags and controls

Table 4.4: Potential financial delegation and asset management red flags and possible controls

Potential red flags	Possible controls
Misuse of delegated financial authority for private gain	
▸ Expenditure that does not align with business needs or approved budgets. ▸ Purchases delivered to private addresses or collected outside normal processes. ▸ Repeated transactions structured just below approval thresholds to avoid scrutiny.	▸ Review transactions against approved budgets and documented business purpose. ▸ Require supporting documentation and additional authorisation for higher-risk purchases. ▸ Escalate recurring or patterned concerns to finance or integrity teams.
Manipulation or concealment of financial records	
▸ Payments regularly coded to vague or catch-all cost centres (e.g. “general services”). ▸ Late cycle adjustments, recoding or journal entries without clear justification. ▸ Repeated amendments by the same individual or business unit.	▸ Require documented rationale and approval for all adjustments and journal entries. ▸ Ensure finance performs independent review of coding and amendments. ▸ Investigate anomalous or repeated changes and escalate where concerns persist.
Misuse or misappropriation of physical assets	
▸ Assets, equipment or supplies frequently missing or unaccounted for. ▸ Use of vehicles, devices or equipment for private business or personal purposes. ▸ Poor visibility over asset location, condition or custody.	▸ Conduct regular asset stocktakes, audits and reconciliations. ▸ Restrict access to high-value or high-risk assets. ▸ Investigate discrepancies promptly and escalate where misuse is suspected.

Grants and funding allocation

Grants and funding programmes present significant corruption risks where employees or decision makers misuse their authority to favour particular applicants, accept improper influence or enable the misuse of public funds. Corruption risks arise where judgement-based decisions lack transparency, personal or external interests influence outcomes, or post-funding oversight is weak, allowing improper conduct to go undetected.

Why risk is higher

- Reliance on subjective assessment, scoring or discretionary judgement in funding decisions.
- High levels of external pressure from applicants, community groups or other stakeholders seeking favourable outcomes.
- Potential for undisclosed personal, professional or community relationships to influence allocation decisions.
- Limited post-funding monitoring and assurance, reducing accountability for how funds are used.
- Weak or inconsistent documentation of assessment scoring and decision-making rationales.
- Opportunities for applicants to misrepresent eligibility, need or intended outcomes, with limited verification.

Red flags and controls

Table 4.5: Potential grant and funding allocation red flags and possible controls

Potential red flags	Possible controls
Suspicious or misleading reporting by funded organisations	
▶ Progress reports lack verifiable evidence of funded activities. ▶ Repeated delays or changes to milestones without credible explanation. ▶ Financial reporting appears inconsistent with approved project scope or budget.	▶ Request supporting evidence such as receipts, deliverables, attendance data and outcomes. ▶ Conduct random post-funding audits or assurance checks. ▶ Withold or suspend further payments until compliance and use of funds are verified.

Potential red flags	Possible controls
Improper influence or pressure from external parties	
▶ External stakeholders or community figures lobby assessors or decision makers on behalf of specific applicants. ▶ Attempts are made to rush assessments, circumvent controls or override established processes. ▶ Offers of gifts, favours, hospitality or other "support" are made during the evaluation process.	▶ Maintain clear boundaries and decline, record and report any offers of benefit. ▶ Document and transparently manage attempts to exert influence or pressure. ▶ Seek advice from integrity, risk or governance teams where pressure persists or escalates.
Applications approved despite not meeting eligibility criteria	
▶ Assessment scores, comments or recommendations do not align with final decisions. ▶ Decisions are altered late in the process without proper documentation or justification.	▶ Require written, criteria-based justification for all funding decisions. ▶ Ensure consistent use of assessment tools, scoring frameworks and moderation processes. ▶ Escalate irregular or unexplained decisions to governance or integrity functions for review.

Regulatory decisions and licensing

Regulatory, licensing and enforcement roles carry significant authority and discretion. Officers exercise delegated authority that directly affect the legal rights, commercial operations and economic outcomes of businesses and individuals.

Corruption risks arise where discretion over approvals, permit conditions, compliance assessments or enforcement responses is misused to solicit or accept improper benefits, tolerate non-compliance or provide unfair advantage to regulated parties. This operational area can be vulnerable to bribery, facilitation payments, conflicts of interest and selective enforcement.

Why risk is higher

- Discretion in interpreting eligibility criteria, compliance requirements and permit conditions.
- Time pressure and applicant urgency that may lead to shortcuts.
- Frequent one-to-one interactions with applicants and regulated parties seeking favourable outcomes.
- High commercial stakes for regulated parties, increasing willingness to offer inducements.
- Direct authority to issue fines, notices, approvals and sanctions with high financial or operational impact on regulated entities.
- Opportunity to misuse confidential information such as inspection timing, assessment criteria or draft conditions.
- Limited supervision for officers working in the field, remotely or independently.
- Risk of repeated contact with the same regulated parties, leading to familiarity or undue influence.

Red flags and controls

Table 4.6: Potential regulatory decision and licensing red flags and possible controls

Potential red flags	Possible controls
Attempts to improperly influence processing or decision making	
▶ Asking an officer to "have a quiet look" and deal with it informally outside a published process. ▶ Using personal or professional relationships to pressure decision makers to deviate from standard criteria or scrutiny.	▶ Decline the approach and explain that all decisions should follow formal processes and criteria. ▶ Record and disclose offers or approaches in accordance with gifts, benefits or code of conduct policies. ▶ Keep all interactions formal and documented.
Ignoring or bypassing mandatory checks	
▶ Required documents or inspections skipped "to save time". ▶ Approvals issued despite outstanding compliance issues. ▶ Backdating compliance steps.	▶ Pause processing until all mandatory requirements are met. ▶ Use checklists, workflow controls or system prompts to enforce mandatory steps. ▶ Escalate pressure to bypass controls to management or integrity functions.

Potential red flags	Possible controls
Misuse or leaking of insider information	
▶ Applicants tipped off about inspection schedules or criteria changes. ▶ Draft permit conditions, compliance thresholds or regulatory requirements shared with an applicant before they are formally issued or made publicly available, allowing the applicant to tailor their submission or adjust their operations ahead of others. ▶ Sensitive information used to shape applications.	▶ Apply need-to-know access controls to systems and sensitive information. ▶ Reinforce confidentiality and privacy obligations through guidance and training. ▶ Audit access logs and investigate suspected unauthorised use or disclosure.
Failing to act where enforcement is required	
▶ Clear breaches identified but no enforcement action is taken. ▶ Pattern of consistent leniency shown to particular individuals or businesses. ▶ Decisions not to act are influenced by personal familiarity or relationships with regulated parties.	▶ Apply legislation, policy and enforcement thresholds consistently. ▶ Record decisions and rationale for action or non-action in official systems. ▶ Escalate patterns of concern to senior management, oversight or integrity functions.

Potential red flags	Possible controls
Offers or attempts to influence inspection outcomes	
▶ Gifts, favours or thank you benefits offered before or after an inspection. ▶ Regulated parties making repeated personal requests for leniency or favourable treatment outside the formal review process. ▶ Suggestions of future work, opportunities or incentives linked to inspection outcomes.	▶ Decline and record all offers or benefits in accordance with conduct policies. ▶ Keep all interactions professional, transparent and fully documented. ▶ Report attempts to influence outcomes to your manager or integrity function immediately.
Improper relationships or familiarity with regulated entities	
▶ Officers repeatedly assigned to the same organisations without rotation or review. ▶ Social contact outside of official interactions that create real or perceived conflicts. ▶ Requests from regulated parties requesting specific inspectors or enforcement employees.	▶ Rotate inspectors and enforcement roles where practicable, especially in high-risk areas. ▶ Maintain professional boundaries and document all official interactions. ▶ Treat requests for specific inspectors as potential influence indicators and escalate for review.

Insider threats and misuse of position

Insider threats arise when employees misuse the access, authority or information their role provides to benefit themselves or others or to cause harm. Insider threats can be difficult to detect, particularly when the conduct occurs within normal work patterns and is perpetrated by trusted employees with legitimate access to systems, data and processes. Insider threat risks exist in every agency, regardless of size or function.

Why the risk is higher

- Employees with privileged system access can retrieve, alter or extract sensitive data without triggering obvious alerts.
- Trust placed in experienced or senior staff can reduce oversight and scrutiny of their conduct.
- High volumes of routine transactions and system activity make deliberate anomalies harder to isolate.
- Employees under financial stress, those with undisclosed outside interests or those who are exposed to, or connected with, foreign interests may be vulnerable to compromise or coercion.
- Weak access controls, absent audit logging or poor segregation of duties can create conditions where insider conduct goes undetected.
- Falsification of records can conceal corrupt activity long after it occurs, making retrospective detection difficult.

Red flags and controls

Table 4.7: Potential insider threat and misuse of position red flags and possible controls

Potential red flags	Possible controls
Misuse of privileged access to systems or data	
▶ An employee accesses records beyond the requirements of their role. ▶ Unusual afterhours or bulk system access occurs without documented business justification. ▶ Queries are run on associates, family members or individuals unrelated to official work. ▶ System access logs show patterns inconsistent with normal job functions.	▶ Apply role-based access controls and review access permissions regularly. ▶ Maintain active audit logging and set alerts for anomalous access patterns. ▶ Ensure access is promptly removed or adjusted when roles change. ▶ Investigate unexplained access patterns rather than treating them as system error.
Unauthorised removal or disclosure of sensitive information	
▶ Large file transfers to personal accounts, removable media or external email addresses occur without authorisation. ▶ An employee with access to classified or commercially sensitive material is financial stress or has recently travelled to high-risk jurisdictions. ▶ Sensitive information appears to have reached external parties who had no legitimate basis to receive it.	▶ Restrict use of removable media and personal email for work files. ▶ Monitor unusual file transfer activity and investigate promptly. ▶ Reinforce confidentiality obligations through employment agreements, training and departure processes.

Potential red flags	Possible controls
Falsification of official records	
▸ Records are amended after decisions have been made with no documented reason. ▸ Gaps or inconsistencies appear in audit trails or document version histories. ▸ Approvals or assessments exist with no supporting documentation. ▸ A single person controls both the creation and storage of records with no independent oversight. ▸ Relevant records are absent, destroyed or unavailable when requested by auditors or reviewers.	▸ Maintain independent oversight of record creation, amendment and storage. ▸ Conduct regular reconciliation of records against decisions and approvals. ▸ Treat unexplained record gaps as a potential integrity concern and assess for escalation, rather than assume there is a system or process issue.
Signs of compromise, coercion or foreign interference	
▸ An employee shows unexplained changes in personal financial position, behaviour or lifestyle inconsistent with their known salary. ▸ Undisclosed foreign connections, travel or contacts are identified. ▸ An employee appears to be under unusual external pressure or exhibits signs of stress, isolation or reluctance to engage with standard oversight processes.	▸ Ensure managers have a clear and accessible pathway to escalate concerns about employee conduct or vulnerability without requiring certainty of wrongdoing. ▸ Apply appropriate pre-employment screening proportionate to the sensitivity of the role. ▸ Agencies whose staff hold security clearances or access nationally sensitive information should consult the New Zealand Security Intelligence Service for guidance on managing foreign interference risks.

External influence and third-party risks

External actors, including lobbyists, contractors, suppliers, former employees and organised criminal networks, can seek to improperly influence agency decisions, exploit third-party relationships or use agency processes to advance private interests. These risks can be more difficult to detect than internal misconduct because the conduct may appear to follow normal business processes and the primary actor operates outside the agency's direct oversight.

Why the risk is higher

- External parties with commercial or political interests in agency decisions have strong incentives to seek improper advantage.
- Third-party and supply chain arrangements can obscure who is actually performing work or receiving public funds.
- Former employees retain insider knowledge of systems, relationships and decision-making processes that can be commercially exploited.
- Informal relationships between current staff and external parties can develop into channels for undue influence.
- Agencies may lack systematic processes for monitoring the conduct of contractors, agents or intermediaries acting on their behalf.

Red flags and controls

Table 4.8: Potential external influence and third-party risk red flags and possible controls

Potential red flags	Possible controls
Third-party and supply chain corruption	
▶ Contractors or subcontractors lack verifiable capability, operational history or a workforce relative to the work they are engaged to perform. ▶ Subcontracting arrangements obscure who is actually delivering services or receiving public funds. ▶ The same individuals or beneficial owners appear across multiple contracted entities. ▶ Due diligence on contractors or agents is limited or absent before engagement. ▶ No integrity or anti-corruption obligations are included in contracts.	▶ Conduct proportionate due diligence on contractors, subcontractors and agents before engagement, including verification of capability and beneficial ownership. ▶ Include integrity and anti-corruption obligations in all contracts. ▶ Maintain oversight of subcontracting arrangements and require notification of material changes to delivery structures.

Potential red flags	Possible controls
Revolving door and post-employment risks	
▸ Senior employees move into roles with organisations they previously regulated, procured from or influenced shortly after leaving. ▸ Former employees engage with their previous agency on behalf of private clients without a cooling-off period. ▸ Jobs, contracts or opportunities are consistently directed to associates or political connections rather than through open competitive processes. ▸ No register of senior departures or post-employment declarations is maintained.	▸ Conduct departure briefings with senior staff covering confidentiality obligations and post-employment restrictions. ▸ Maintain a register of senior departures and declared post-employment arrangements. ▸ Treat former employee engagement on behalf of external clients as a potential conflict of interest and manage accordingly.

Criminal infiltration and institutional money laundering

Organised criminal networks may deliberately seek to place individuals within agencies or exploit agency payment and contracting processes to move or conceal funds. These risks require specialist assessment and response. Agencies that believe they have identified indicators of organised criminal involvement, or suspicious transaction patterns related to such involvement in outgoing payments, should contact the New Zealand Police.

5

Countering corruption

Prevention is often more effective and less costly than responding after harm has occurred. Corruption prevention should be considered as a system that brings together leadership commitment, sound risk assessment, well-designed controls and a culture where integrity is the norm.[11]

This chapter sets out a potential strategic framework for effective corruption control, structured around four reinforcing categories: capability, prevention, detection and response. Each category serves a distinct purpose, and none is sufficient on its own. Together, they form a coherent system based on foundational principles of effective corruption prevention. The chapter highlights priority domains that may require focused attention and concludes with potential tools to assess if corruption prevention measures are working.

Corruption control categories

Capability

Capability shapes how people understand, internalise and apply integrity expectations in their day-to-day work. It is built through clear guidance, practical training, leadership and the active modelling of ethical behaviour. Social norms matter. When employees see that integrity is expected, reinforced and demonstrated by leaders and peers it weakens rationalisations such as “everyone else is doing it” and makes corruption less likely to take hold.

[11] See https://www.publicservice.govt.nz/guidance/the-code-of-conduct-for-the-public-sector.

Prevention

Prevention is the first line of defence. It primarily reduces the opportunity for corruption by designing systems, processes and controls that limit unchecked discretion, increase transparency and embed proportionate controls into everyday operations. Effective prevention does not rely on trust alone. It anticipates where risks arise and uses sound design to make improper behaviour more difficult, more visible and less rewarding.

Detection

No prevention system is flawless. Detection ensures that when corruption does occur, it is identified early, limiting harm and enabling a timely intervention. Effective detection relies on multiple reinforcing mechanisms, including data analytics, audit trails, behavioural indicators and a reporting culture where people feel safe to speak up.

A significant proportion of corruption is uncovered through tip offs and disclosures rather than routine audits or data analysis. This makes it essential to have accessible and credible reporting pathways, including avenues for anonymous reporting. Detection must also be visible. When employees know that monitoring is active and controls operate in practice, detection strengthens both early intervention and deterrence.

Response

When corruption is identified or suspected, the response must be prompt, consistent and proportionate. Clear process should set out how concerns are assessed, how evidence is secured and how matters are escalated – whether through internal investigation, disciplinary action or referral to law enforcement.

An effective response reinforces the entire framework. It demonstrates that standards are applied in practice, strengthens deterrence and builds confidence among employees that raising concerns will lead to fair, credible and protective outcomes. Addressing both minor and serious breaches of integrity is essential. Left unchecked, small violations can signal tolerance, contributing to the normalisation of improper practices and their gradual escalation over time.

Corruption control principles

The following principles form the structural foundation of an effective corruption control framework. They reflect widely recognised international practice and can apply to any New Zealand public sector organisation. The principles work best when treated as a connected system rather than isolated elements.

Proportionate procedures

Prevention measures should match an organisation's size, risk profile and operating environment. Procedures work best when built into everyday practice rather than treated as standalone compliance tasks. They should be practical, easy to understand and applied consistently.

Examples

- Align procurement checks with contract value, applying more scrutiny to higher-risk purchases.
- Design simple conflict of interest processes for small teams and more formal processes for large, high-risk functions.
- Integrate key controls (such as approval steps) into everyday workflows rather than creating extra layers of paperwork.

Top level commitment

Leadership shapes the ethical tone of an organisation. Commitment at the top involves transparent decision making, consistent standards and active engagement with integrity issues. Employees tend to take stronger cues from what leaders do than from what policies say. Visible integrity at senior levels is one of the strongest organisational deterrents to corrupt behaviour.

Examples

- Senior leaders regularly reinforce integrity expectations in team meetings, staff updates and decision-making discussions.
- Leaders disclose their own conflicts of interest openly and model how to manage them.
- Leadership responds promptly and transparently when concerns about corruption are raised.

Risk assessment

A structured risk assessment identifies corruption risks across functions and roles, assesses their likelihood and impact, identifies and reviews existing controls, and highlights areas needing attention. Risk assessments should be reviewed regularly and updated when significant changes occur, such as new programmes, organisational restructures or shifts in the external environment. They work best when a senior leader is accountable for them and they are kept up to date as risks, roles and controls change over time.

Examples

- Map corruption risks across functions such as procurement, grants, recruitment and regulatory activity.
- Hold workshops with teams to identify practical vulnerabilities and test assumptions about risk.
- Update risk assessments when launching a new programme, entering new partnerships or changing organisational structure.

Due diligence

Organisations benefit from understanding who they work with, especially when third parties act on their behalf or hold ongoing influence. Due diligence should be proportionate to the nature of the relationship and the risks involved. It is most effective when revisited over time, particularly when circumstances change.

Minimum due diligence may include identity checks, sanctions screening and basic integrity assessments. Enhanced due diligence may involve deeper background checks, financial and capability analysis, media review or reference verification for higher risk or high value relationships.

Examples

- Verify the identity, ownership and basic integrity history of new suppliers before entering contracts.
- Conduct enhanced checks on high risk partners, such as overseas vendors or intermediaries with access to sensitive information.
- Reassess existing suppliers periodically, especially when invoices, behaviour or circumstances change.

Communication and training

Employees need a clear understanding of what corruption looks like in their context, the red flags and warning signs to watch for, and what to do if they have concerns. Awareness should be tailored to the level of risk in each role, with more detailed guidance for staff in high-risk areas. All employees should know how to raise concerns and the protections available to them.

Examples

- Provide induction training that explains corruption risks relevant to the organisation's work.
- Run targeted sessions for high risk teams such as procurement, grants, licensing or regulatory enforcement.
- Share short case studies or alerts when emerging risks or patterns are identified.

Monitoring and review

Prevention measures should be monitored and reviewed regularly, looking at patterns in declarations, reviewing due diligence outcomes, testing the effectiveness of controls and examining themes in reported concerns. Monitoring needs to be active and analytical. Trends in gifts and hospitality, procurement decisions or conflict of interest disclosures can reveal emerging risks early.

Examples

- Review gifts, hospitality and conflict of interest registers to identify unusual patterns.
- Periodically run data analytics on procurement activity to detect anomalies such as repeated awards to the same supplier.
- Follow up on themes that appear in internal reports or staff concerns to test whether controls are working effectively.

Corruption control priority domains

Effective counter corruption efforts require a deliberate, risk-based approach that directs resources to the areas of greatest vulnerability. All controls will have a cost – financial, staff time or operational complexity – so consider prioritising action in high-risk processes and finding the appropriate balance between mitigating the corruption risk and the resource investment required.

Conflicts of interest

Conflicts of interest are one of the most common and significant risk factors in the public sector and feature in many corruption cases. Conflicts of interest often sit beneath other forms of misconduct, including the acceptance of improper benefits, misuse of resources, fraud and deception, abuse of power and influence peddling.

Because conflicts of interest frequently arise before misconduct occurs, they are a critical point for prevention. When identified early and managed effectively, they can be addressed without harm. When they are not disclosed or are poorly managed, they can allow corruption to develop and become more difficult to detect.

Conflicts of interest are sometimes treated as an administrative exercise, such as completing a form or maintaining a register. The Public Service Commission conflicts of interest model standards emphasise that all public sector organisations should integrate conflict of interest management with their human resources, employment relations and operational management systems.[12]

Control example

Clear and mandatory disclosure framework

Employees should disclose financial interests, personal relationships, outside roles and any situation that could influence or appear to influence their judgement. Disclosures should be timely and made when the conflict arises.

- Declaration of a family connection with a supplier before procurement planning begins.

[12] See https://www.publicservice.govt.nz/guidance/model-standards-conflicts-of-interest/conflicts-of-interest-model-standards.

Control example

Registration and active management

Once a conflict is declared, there should be a documented decision about how to manage it, such as recusal, reassignment or additional oversight. Maintaining a register alone does little to mitigate risk.

- A manager allocates oversight of a procurement process to someone independent of the conflict.

Control example

Culture of early transparency

Employees should feel safe raising potential conflicts early, even when they are unsure whether a situation constitutes a conflict. Encouraging early disclosure helps prevent minor issues from becoming significant risks.

- Staff routinely check with managers when unsure whether a situation may pose a conflict of interest.

Possible actions

- Maintain a conflict of interest register that records disclosures, decisions and outcomes, not just declarations.
- Require disclosure at the start of employment, at regular intervals and whenever a new conflict arises.
- Ensure every declared conflict has a documented management strategy with heightened scrutiny where senior staff, procurement, appointments or funding decisions are involved.
- Create a clear, accessible process that allows staff to raise potential conflicts early without fear of negative consequences.

Third-party and supply chain risk

Suppliers, contractors, consultants, agents, subcontractors and grant recipients can all expose an organisation to corruption risk even when internal controls are strong. This risk has two dimensions: third parties may engage in corrupt conduct connected to the organisation's work, and they may attempt to influence employees through gifts, hospitality, kickbacks or other inducements. Managing this risk calls for active oversight by those responsible for establishing and managing third party relationships before, during and after engagement.

Control examples

Before engagement: due diligence

Before entering into a significant or higher-risk relationship, due diligence should be applied in a way that is proportionate to the level of risk. The degree of scrutiny can reflect factors such as contract value, the nature of the work, where the third party operates and any indicators of elevated risk.

- Confirm the identity of a new supplier and check for sanctions or known integrity issues.
- Require prospective partners to declare any personal, financial or governance links to organisation staff.

Control examples

During the relationship: ongoing oversight

Third-party risk changes over time. A supplier initially assessed as low-risk may undergo new ownership, face financial pressure or begin operating in higher-risk environments. Oversight should be active and built into the relationship.

- Conduct regular performance and compliance reviews, including spot checks where appropriate.
- Verify that subcontractors meet the same integrity expectations as primary suppliers.

Control examples

After the relationship: managing residual risk

When a significant relationship ends, organisations should ensure that any residual risks or obligations do not continue unnoticed.

- Confirm that confidential information shared during the contract has been returned or securely destroyed.
- Remind staff who worked closely with the supplier of their ongoing obligations, including post employment restrictions.

Possible actions

- Map significant third party relationships and assess the corruption risk associated with each.

- Tier due diligence requirements so that higher-risk relationships receive deeper scrutiny.
- Review contracts to ensure they include anti corruption expectations, audit rights and termination options for integrity failures.
- Provide staff with a safe, accessible way to raise concerns about third-party behaviour.

Insider threat

Insider threat is widely recognised as a significant but often overlooked corruption risk in the public sector. It refers to the risk that people already inside an organisation may misuse the access, authority or information their role provides for private gain. When someone understands a process well, they can exploit discretion or control gaps in ways that are hard to identify, sometimes over long periods, until serious harm has occurred. Managing insider threats calls for thoughtful decisions about how trust is structured and supported by verification, oversight and accountability across the organisation.

Control example

Roles, access and separation of duties

The most effective structural defence against insider threats is to make sure no single person has end-to-end control over a high-risk or high-value process. Segregation of duties, such as splitting up initiation, approval and review functions, reduces the likelihood that one person can act alone.

At a strategic level, organisations can work to identify where a single person has end to end decision making power over a high-value or high-risk activity. These are key vulnerability areas and can be addressed by tools like structural separation or compensating controls, such as dual sign off, independent review or automated audit trails. When corrupt activities require collusion, it becomes significantly harder to initiate and sustain in an undetected way.

- Separate initiation and approval roles so one person cannot both raise and approve a payment.
- Require two independent reviewers for high-value contracts or sensitive decisions.

Control example

High-risk roles and targeted oversight

A key defence against insider threat is the deliberate identification and oversight of roles with elevated corruption exposure. These roles typically involve significant authority and limited oversight, access to sensitive information or unsupervised interaction with external parties. They commonly include procurement teams, financial system administrators, licensing and enforcement officers, and roles with access to confidential intelligence or personal data. Organisations can reduce this risk by proactively identifying high-risk roles and applying oversight mechanisms proportionate to the level of exposure.

- Rotate staff in procurement or financial administration roles at planned intervals.
- Require regular conflict of interest refreshes for roles with high external contact.
- Conduct periodic supervision or sampling checks on case files handled by field staff.

Possible actions

- Map the organisation's highest-risk roles and periodically assess whether separation of duties and oversight remain adequate.
- Identify processes where a single person has full control and introduce appropriate compensating controls where separation is not feasible.
- Build rotation of high-risk roles into workforce planning where practicable.
- Support managers to intervene early when small boundary issues arise – these moments are preventative, not overreaction.

Post employment and revolving door

Some of the least visible corruption risks arise after a person leaves public service. When senior public officials move into private sector roles with organisations they previously regulated, oversaw or awarded contracts to, the integrity of their earlier decisions may be questioned even when no misconduct occurred.

This movement between public and private roles, often referred to as the revolving door, creates risks in both directions. Public sector employees may shape decisions with future employment in mind, for example, a senior procurement employee joining a major supplier shortly after awarding that supplier a significant contract. Conversely, private sector leaders entering public roles may favour former employers or professional associates.

These risks are subtle and difficult to detect. The core issue is the potential use of insider knowledge, relationships or influence gained in one role being transferred to the next. By the time such patterns become visible, opportunities for effective intervention are often limited. Effective management of post employment risk calls for controls to be established before departure, not after. It is fundamental that such controls must always comply with relevant employment laws.

Control example

Cooling-off periods

Cooling off periods restrict senior or high-risk employees from accepting certain roles for a defined period after leaving the public service. The length and scope should be proportionate to the seniority of the role, the nature of the decisions made and the level of influence it carried.

- Require a six-month restriction on joining organisations that were directly regulated or contracted by the employee's former business unit.

Control example

Disclosure and approval requirements

Employees in senior or high-risk roles could be required to disclose, and in some cases seek approval for, job offers that may create a real or perceived conflict with their public duties. Depending on the role, these requirements may apply for a defined period after departure.

- Record decisions, conditions and advice relating to post employment disclosures for future reference.

Control example

Departure briefings

Employees leaving high-risk roles should receive clear, documented advice about their ongoing obligations, including confidentiality requirements, conflict of interest expectations and any applicable, lawful, post employment restrictions.

- Require written acknowledgement of confidentiality obligations and post employment conditions at the point of departure.

Control example

Register of senior departures

Maintaining visibility over where senior employees move to after leaving can help identify emerging trends or integrity risks, particularly where former employees join a company that had significant dealings with the public sector organisation.

- Flag departures that may require follow up, such as joining a major supplier soon after contract negotiations or regulatory decisions.

Possible actions

- Review whether employment policies include clear post employment expectations for senior and high-risk roles.
- Ensure cooling-off periods are defined, proportionate, clearly communicated and applied consistently and legally.
- Consider whether your organisation has adequate visibility over senior departures and whether emerging patterns warrant attention.

Assessing corruption prevention measures

A prevention framework must be assessed to be improved. Corruption prevention is difficult to measure because the absence of incidents does not, on its own, demonstrate that controls are effective. An organisation may report few cases, however, this does not necessarily mean risk is low – perhaps detection is weak, reporting is discouraged or risks have not yet surfaced.

Collect actionable data

Agencies should collect and record information accurately and consistently. Clear categorisation of alleged or proven wrongdoing, alongside details of actual or estimated losses, enable integrity staff to analyse trends, impacts and recurrence over time. This allows organisations to better assess whether prevention activities are reducing both the likelihood and consequences of misconduct.

Excessive use of categories such as “not applicable” or “unknown” limits the ability to distinguish between minor issues and more serious misconduct. Poor data quality is itself a risk indicator. When cases are recorded inconsistently or without sufficient detail, an organisation loses visibility of its true risk profile.

Use leading and lagging indicators

Meaningful measurement requires both leading indicators that show how the system is operating before problems occur and lagging indicators that record what has already happened. Neither will be sufficient on its own.

Example

Leading indicators: how the system is functioning

Leading indicators provide insight into whether prevention measures are being applied as intended and whether integrity settings are embedded in day-to-day operations.

- Training completion rates, particularly when training is tailored to different risk levels or roles.
- Trends in declarations for gifts, hospitality, conflicts of interest and secondary employment. A sudden decline may indicate cultural or reporting issues rather than reduced risk.
- The proportion of declarations that result in documented management actions.
- The volume and nature of issues raised through reporting channels, including near misses.
- Completion rates for due diligence on new and existing third party relationships and the proportion assessed as higher risk.
- Results of control testing under real operating conditions, not just in theory.

Example

Lagging indicators: what has happened

Lagging indicators reflect the outcomes the prevention controls are designed to avoid. While they should not be used as the sole measure of success, they provide important context and learning.

- The number, type and outcome of corruption or fraud investigations.
- Disciplinary cases involving integrity breaches, including those not formally labelled as corruption.
- Audit findings identifying control weaknesses, particularly where issues persisted over time.
- Findings from external reviews, Ombudsman investigations or regulatory actions.

Undertake reporting and assurance

Measurement insights must reach decision makers who are able to act on them. Governance bodies, boards, audit and risk committees, and senior leadership should receive regular, meaningful reporting on the health of the corruption prevention system.

Effective reporting goes beyond point-in-time compliance statistics to highlight trends, patterns, emerging risks and honest assessments of both strengths and weaknesses. The maturity and candour of assurance reporting is itself a sign of organisational integrity.

The goal of corruption prevention is not zero incidents. It is a system that identifies risks early, responds proportionately and learns from both near misses and confirmed cases. To prove prevention is functioning as a strategic capability, agencies should consider if they are able to report on incidents and on the condition of the systems designed to prevent them.

Possible actions

- Define a balanced set of leading and lagging indicators and report on them regularly.
- Provide governance bodies with clear snapshots of current performance alongside trends that show whether outcomes are improving or worsening.
- Assess whether low levels of declarations or reports reflect genuinely low risk or cultural barriers to reporting.
- Use audit and review findings to test whether controls operate effectively in practice, not only whether they exist on paper.

6

Conclusion

Corruption takes hold gradually, often through small compromises, unchecked conflicts and relationships that blur professional boundaries. There is no single solution to managing corruption risks, and prevention approaches must continually adapt to address evolving threats.

The most effective response is preventive: building systems, culture and everyday practices that make corrupt conduct harder to initiate, easier to detect and less likely to be tolerated. Organisations can considerably reduce and manage their risk of corruption by:

- understanding why corruption occurs and how individuals can be drawn into it
- recognising common corruption risks and behaviours
- assessing where corruption is most likely to occur in their organisation
- putting in place effective checks and balances
- monitoring, reporting and continuously improving their approach.

No system eliminates corruption entirely. However, organisations that invest in prevention are better placed to protect public resources, maintain public trust and respond effectively when problems do arise.

Appendix: Key operational risk areas for corruption

This table maps the forms of corruption identified in chapter three against the key operational risk areas in chapter four. Each cell shows how that form of corruption can typically manifest in that context. In practice, corrupt conduct often spans multiple categories simultaneously. Note, this mapping is intended as a recognition and awareness tool. The presence of one form of corruption may indicate related risks in adjacent categories as corruption is rarely isolated.

Form of corruption	Key operational risk area							
	Procurement and contract management	Recruitment, appointments and payroll	Secondary employment	Financial delegations and asset management	Grants and funding allocation	Regulatory decisions and licensing	Insider threats and misuse of position	External influence and third-party risks
Abuse of power and influence peddling	Bypassing procurement rules	Influencing panel decisions or approving payroll changes under duress	Pressuring staff to conceal outside work or undeclared interest	Ignoring financial controls	Fast-tracking favoured applicants	Overriding eligibility criteria or directing altered inspection outcomes	Overriding system controls, including self-approval in breach of segregation of duties	Lobbying, pressure or influence from external parties affecting decisions
Improper benefits	Kickbacks or hospitality during tenders	Job offers or payments in exchange for recruitment selection or approval of inflated hours	Benefits offered to overlook undeclared conflicts of interest or outside work	Payments to approve invoices or spending	Payments to secure funding approval	Payments to fast-track permits or avoid penalties	Payments to disclose sensitive information	Gifts, hospitality or inducements from third parties to influence outcomes

Form of corruption	Key operational risk area							
Exploited or undisclosed conflicts of interest	Undeclared personal or financial relationships with suppliers	Hiring relatives or friends or approving payroll for associates	Undisclosed business interests in same sector	Awarding contracts to related parties	Funding decisions involving connected organisations	Approving applications from associates or overlooking breaches involving known parties	Undeclared personal or financial relationships influencing decisions or access to sensitive information	External parties influencing decisions through relationships with employees
Misuse of resources	Inflated contracts or phantom deliverables	Payroll manipulation or ghost workers	Using organisational time, systems or assets to support secondary employment or private business activities	False expense claims or misuse of purchasing cards	Diverting grant funds	Misusing regulatory resources, including charging private costs to regulatory budgets or unauthorised use of enforcement assets	Unauthorised use of systems or data for personal gain	Third parties using organisational resources via employee access (e.g. facilities, systems or equipment)
Fraud and deception	False invoices or forged contract variations	Fake qualifications, fraudulent references or altered payroll records	Falsified declarations of outside interests	Falsified financial statements or journals	Fabricated funding reports or milestone claims	Altered application documents or manipulated inspection records	Falsifying records, audit logs or system inputs to conceal activity	Using shell companies or false documentation

Form of corruption	Key operational risk area							
Misuse of information	Sharing competitor bids or tender details	Sharing interview questions, candidate data or payroll records without authority	Using confidential organisational knowledge to benefit external or secondary employment	Disclosing sensitive financial data	Leaking funding criteria or applicant information	Revealing application or inspection status or alerting regulated parties to upcoming audits	Unauthorised access, extraction or disclosure of sensitive or classified information	Third parties exploiting relationships with employees to obtain restricted information
Collusion and market manipulation	Bid rigging or price fixing among suppliers	Predetermined recruitment outcomes or collusive payroll approval transactions (e.g. timesheets, allowances)	Coordinated efforts by employees to hide outside work	Coordinated manipulation of budgets or records	Coordinated funding applications to manipulate eligibility or approval outcomes	Coordinated permit approvals or enforcement avoidance	Using insider access to assist external parties	Coordination among external suppliers to manipulate process or outcomes
Concealment of proceeds of crime	Recording bribes as consultancy fees	Hidden payments routed through payroll or concealed through altered records	Concealing income or benefits from secondary employment, including undeclared payments or conflicts	Routing corrupt funds through shell entities	Disguising kickbacks in grant payments	Coding improper payments as permit fees or altering enforcement records to hide misconduct	Altering or deleting records to hide improper access, transactions or data leakage	Using intermediaries, subcontracting or layered arrangements to disguise activity

Form of corruption	Key operational risk area							
Affiliation and patronage practices	Awarding contracts before moving to a supplier	Making appointments based on loyalty rather than merit or overlooking payroll issues for favoured staff	Approving outside work for future employers	Favouring past business associates in spending decisions	Funding organisations linked to future employment	Preferential treatment of former employers or lenient oversight of former colleagues	Using knowledge or access to benefit future employment or external affiliations	External parties engaging recently departed employees to gain preferential access or insight into organisation's processes

8

References

Anderson, E., 2013. Municipal “best practices”: Preventing fraud, bribery and corruption. Canada: International Centre for Criminal Law Reform and Criminal Justice Policy. https://icclr.org/wp-content/uploads/2019/06/Municipal-Best-Practices-Preventing-Fraud-Bribery-and-Corruption-FINAL.pdf.

Controller and Auditor-General, 2020. Managing conflicts of interest: A guide for the public sector. Wellington: Office of the Auditor-General. https://oag.parliament.nz/2020/conflicts.

Controller and Auditor-General, 2024. Putting integrity at the core of how public organisations operate: An integrity framework for the public sector – second edition. Wellington: Office of the Auditor-General. https://oag.parliament.nz/2024/integrity-framework/preface.htm.

Corrupt Practices Investigation Bureau, 2017. PACT: A practical anti-corruption guide for businesses in Singapore. Singapore: Corrupt Practices Investigation Bureau. https://www.cpib.gov.sg/research-room/publications/anti-corruption-guide-for-businesses/.

Counter Fraud Centre, 2025. Procurement fraud and corruption risk: Building fraud and corruption prevention capability and culture in the public sector. Wellington: Serious Fraud Office. https://www.sfo.govt.nz/counter-fraud/guidance/procurement-fraud-and-corruption-risk.

Government Counter Fraud Function, 2021. New Zealand Serious Fraud Office Counter Fraud Centre: Fraud loss in the New Zealand public sector. London: Government Counter Fraud Function. https://www.sfo.govt.nz/publications/proactive-information-releases.

Government Counter Fraud Profession Centre of Learning, 2024. How to counter bribery and corruption: Practice note. London: Public Sector Fraud Authority. https://www.gov.uk/government/publications/how-to-counter-bribery-and-corruption-practice-note.

Minkova, M., 2018. Guide to corruption-free local government. New York: United Nations Development Programme Europe and Central Asia. https://www.undp.org/eurasia/publications/guide-corruption-free-local-government.

New South Wales Independent Commission Against Corruption, 2018. Strengthening employment screening practices in the NSW public sector. Sydney: New South Wales Independent Commission Against Corruption. https://www.icac.nsw.gov.au/media-centre/media-releases/2018-media-releases/icac-recommends-nsw-public-sector-tighten-screening-practices-to-combat-employment-application-fraud-and-corruption.

New South Wales Independent Commission Against Corruption, 2020. Dealing with corruption, fraud and the ICAC: The role of public sector audit and risk committees. Sydney: New South Wales Independent Commission Against Corruption. https://www.icac.nsw.gov.au/prevention/corruption-prevention-publications/latest-corruption-prevention-publications/dealing-with-corruption-fraud-and-the-icac-the-role-of-public-sector-audit-and-risk-committees.

New South Wales Independent Commission Against Corruption, 2022. Managing corruption risks in regulatory work. Sydney: New South Wales Independent Commission Against Corruption. https://www.icac.nsw.gov.au/about-the-nsw-icac/nsw-icac-publications/all-nsw-icac-publications/managing-corruption-risks-in-regulatory-work.

New South Wales Independent Commission Against Corruption, 2023. Fraud and corruption control: Evaluating compliance and its drivers. Sydney: New South Wales Independent Commission Against Corruption. https://www.icac.nsw.gov.au/prevention/corruption-prevention-publications/latest-corruption-prevention-publications/fraud-and-corruption-control-evaluating-compliance-and-its-drivers-november-2023.

New South Wales Independent Commission Against Corruption, 2023. Mature corruption control: The key outcomes of better practice. Sydney: New South Wales Independent Commission Against Corruption. https://www.icac.nsw.gov.au/prevention/corruption-prevention-publications/latest-corruption-prevention-publications/mature-corruption-control-the-key-outcomes-of-better-practice-march-2023.

New South Wales Independent Commission Against Corruption, 2024. Common forms of corrupt conduct: Risks faced by NSW public sector agencies. Sydney: New South Wales Independent Commission Against Corruption. https://www.icac.nsw.gov.au/prevention/corruption-prevention-publications/latest-corruption-prevention-publications/common-forms-of-corrupt-conduct-risks-faced-by-nsw-public-sector-agencies-june-2024.

New South Wales Independent Commission Against Corruption, 2025. Coerced, compromised or groomed: How people get drawn into corrupt conduct. Sydney: New South Wales Independent Commission Against Corruption. https://www.icac.nsw.gov.au/prevention/corruption-prevention-publications/latest-corruption-prevention-publications/coerced-compromised-or-groomed-how-people-get-drawn-into-corrupt-conduct-june-2025.

Northern Ireland Audit Office, 2017. Managing the risk of bribery and corruption: A good practice guide for the Northern Ireland public sector. Belfast: Northern Ireland Audit Office. https://www.niauditoffice.gov.uk/publications/managing-risk-bribery-and-corruption.

Organisation for Economic Co-operation and Development and United Nations, 2024. A resource guide on state measures for strengthening business integrity. Paris: OECD Publishing and New York: United Nations. https://www.oecd.org/en/publications/resource-guide-on-state-measures-for-strengthening-business-integrity_c76d7513-en.html.

Organisation for Economic Co-operation and Development, 2026. Anti-corruption and integrity outlook 2026: Harnessing the integrity advantage. Paris: OECD Publishing. https://www.oecd.org/en/publications/anti-corruption-and-integrity-outlook-2026_16708b78-en/full-report/component-14.html#chapter-d1e13113-f9ebfc554e.

Te Kawa Mataaho Public Service Commission, 2025. Model standards: Conflicts of interest. Wellington: Te Kawa Mataaho Public Service Commission. https://www.publicservice.govt.nz/guidance/model-standards-conflicts-of-interest.

Te Kawa Mataaho Public Service Commission, 2026. Te tauākī whanonga mō te rāngai tūmatanui | The code of conduct for the public sector. Wellington: Te Kawa Mataaho Public Service Commission. https://www.publicservice.govt.nz/guidance/the-code-of-conduct-for-the-public-sector.

Transparency International, 2014. Using the UN Convention Against Corruption to advance anti-corruption efforts: A guide. Berlin: Transparency International and UNCAC Coalition. https://www.transparency.org/en/publications/guide-using-uncac-to-advance-anti-corruption-efforts.

Transparency International, 2025. Follow the money – TINZ corruption scan March 2025. https://www.transparency.org.nz/blog/follow-the-money---tinz-corruption-scan-march-2025 [accessed 30 March 2026].

Transparency International, 2025. Why the shift downwards? https://www.transparency.org.nz/blog/why-the-shift-downwards [accessed 30 March 2026].

United Nations Global Compact, 2009. Reporting guidance on the 10th principle against corruption. Berlin: United Nations Global Impact and Transparency International. https://unglobalcompact.org/library/154.

New Zealand Government
Te Kāwanatanga o Aotearoa

The Serious Fraud Office Te Tari Hara Tāware is the lead law enforcement agency for investigating and prosecuting serious or complex fraud, including bribery and corruption. It works to strengthen the public sector's resilience to fraud and corruption through its Counter Fraud Centre Tauārai Hara Tāware.

June 2026

SFO
SERIOUS FRAUD OFFICE
TE TARI HARA TĀWARE

Counter Fraud Centre
TAUĀRAI HARA TĀWARE