New Zealand Government
Te Kāwanatanga o Aotearoa

Fraud control catalogue

Capability, prevention, detection and response controls to mitigate the risk of fraud and corruption in public sector organisations

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

	Introduction	**4**
	Who this resource is for	5
	How to use this catalogue	5
	**Capability controls**	**7**
	Defined decision-making powers	8
	Ethical culture	10
	Governance and oversight	12
	Help and support	14
	Managerial or independent oversight	16
	Strategic partnerships	18
	Sufficient resourcing	20
	Trained and qualified employees	22
	**Prevention controls**	**24**
	Access controls	25
	Accurate information collection	28
	Accurate information maintenance	31
	Approval workflows	33
	Automatic prompts and alerts	35
	Change management processes	37
	Compliance, performance and contract reviews	40
	Contractual clauses	42
	Counter fraud messaging	44
	Data protection	46
	Declarations	48

Decommissioning and disposal 50
Disclosure and reporting 53
Duplicate prevention 55
Eligibility requirements 57
Employee and contractor rotation 60
Escalation procedures 62
Fraud awareness training 64
Identity verification 66
Integrity checks and suitability assessments 68
Mandatory information 71
Parameters and limits 73
Policies 75
Privileged system access 77
Procedural instructions or guidance 80
Public transparency 82
Random allocation 84
Segregation of duties 86
Sensitive information access 89
Sensitive information control 91
Specific and consistent processes 94
System testing 96
User permissions 98
Watchlists 101

Detection controls 103

Activity reporting 104

Automatic change notifications 106

Automatic data matching 108

Avenues for reporting fraud 110

Complaints handling 112

Evidence and document capture and storage 114

Exception reporting 116

Fraud detection software 118

Incident reporting 120

Information verification 122

Internal audits or reviews 124

Quality assurance checks 126

Record reconciliation 128

Response controls 130

Audit logging 131

Coordinated disruption activity 133

Fraud investigation policy 135

Penalties for fraud and non-compliance 137

Recovery and debt management processes 139

Separation and termination processes 141

Build capability and culture 143

Introduction

Fraud is when someone deliberately deceives others, often hiding what they are doing, to gain an advantage or benefit or cause loss to another. Because of this, organisations are encouraged to implement a range of counter fraud and corruption controls (or countermeasures) to minimise opportunities to commit fraud and maximise the likelihood of detection.

Fraud risks can be managed by putting in place practices and controls to mitigate the risks or by designing specific fraud evaluation procedures. The appropriate mix of controls will vary depending on an organisation's risk exposure, operating environment and tolerance for risk.

No system of controls can completely eliminate fraud. However, well designed and effectively implemented controls significantly enhance an organisation's ability to prevent, detect and respond to fraudulent behaviour.

Controls typically fall into four categories:

- **Capability controls** guide expected behaviours and determine organisational culture around fraud. They provide clarity and direction for employees.
- **Prevention controls** are the most common and cost-effective interventions, reducing the likelihood of fraud occurring by limiting opportunities for fraudsters.
- **Detection controls** support the timely identification of fraud, enabling organisations to disrupt activity and reduce the impact of it occurring.
- **Response controls** are activated after fraud has occurred to contain further harm. These controls include investigation, prosecution, disciplinary action and recovery activities.

Who this resource is for

This catalogue is intended for anyone involved in managing, responding to or overseeing fraud and corruption risks. It supports employees at all levels, including operational teams, risk managers, senior leaders and governance groups, who need to understand effective controls and how they can be applied within their organisation.

How to use this catalogue

This guidance does not provide an exhaustive list of controls, nor one-size-fits-all solutions. It is designed to be a practical starting point to help organisations strengthen their fraud and corruption control environment in a way that is proportionate to their risk profile.

This document lists controls in alphabetical order, by category. It can be read in any order, as the organisation's control environment evolves.

Organisations can use this catalogue to:

- **Identify and understand available fraud control options**

  Review the controls listed in the catalogue to understand the range of capability, prevention, detection and response controls that may be used to address fraud and corruption risks.

- **See examples of the control in action**

  Review illustrative examples that show how the control could be implemented in your organisation.

- **Understand the risks of control gaps**

  Understand why each control is important and the potential fraud, corruption or integrity risks that may arise if the control is absent or ineffective.

- **Assess whether existing controls are operating effectively**

  Identify ways to test whether existing controls are implemented, operating as intended and achieving their intended outcomes.

- **Identify complementary controls to strengthen the control environment**

  See a range of additional controls that may enhance effectiveness, provide layered protection or address weaknesses in the existing control framework.

- **Identify controls relevant to specific fraudster personas**

  Learn which behaviours posed by particular fraudster types may be mitigated by the control.

Some controls also refer to the Protective Security Requirements, which is a policy framework that outlines the Government's expectations for managing personnel, physical and information security.

Organisations should apply professional judgement when using this catalogue, and tailor the selection and application of controls to their specific risk exposure, operating environment and tolerance for risk.

Capability controls

Capability controls establish the organisational foundation for effective fraud prevention and management by setting the tone from the top. They focus on building and sustaining an ethical culture grounded in transparency, accountability and integrity, ensuring that expectations around conduct are clearly understood across the organisation.

These controls require leaders to consistently model expected behaviours and demonstrate a visible commitment to ethical decision making and zero tolerance for fraud. They also ensure that roles, responsibilities and accountabilities are clearly defined, enabling staff to understand their part in preventing, detecting and responding to fraud risks.

Defined decision-making powers

Clearly define decision-making powers to increase transparency and reduce the opportunity for fraud and corruption.

This control targets internal fraud risks.

Examples

Examples of this control include:

- financial delegations, e.g. requiring international travel to be approved by a senior employee
- human resource delegations, e.g. approving leave and entitlements
- procedures that define who can make decisions, e.g. requiring managerial approval to change a vendor's bank account
- clear responsibility for decision making in joint or multiagency programmes.

Risks from control gap

A lack of clarity for decision-making powers can lead to:

- high levels of non-compliance or errors due to inconsistent practices
- common use of shortcuts and workarounds
- a lack of transparency over actions and decisions
- poor management of fraud and corruption risks
- fraudsters not obtaining approval or obtaining approval from someone who is not the appropriate decision maker
- fraud or corrupt activity going unnoticed or unchallenged
- unknown and unaddressed systemic fraud or corruption.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that delegation documents exist, are current and comply with relevant legislation , policies and guidelines
- undertaking testing or a process walkthrough to confirm that processes cannot be avoided or bypassed when subjected to pressure or coercion

- reviewing a sample of approval decisions to determine whether processes and workflows are followed on all occasions
- identifying how the requirement to follow specified decision-making processes are communicated to employees.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Approval workflows
- Governance and oversight
- Policies
- Procedural instructions or guidance
- Public transparency

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The enabler
- The exploiter

Ethical culture

Create an ethical culture that encourages supportive behaviours, while discouraging potentially fraudulent or corrupt activities.

This control targets internal fraud risks.

Examples

Examples of this control include:

- integrated organisational values in day-to-day activities
- reward and recognition programmes
- health and wellbeing training and initiatives
- an inclusive and supportive workplace culture
- training in and promoting ethical conduct and decision making
- leaders demonstrate ethical behaviour by adhering to procedures and being held accountable in the same way as all employees
- open and transparent communication and decision making.

Risks from control gap

An unethical workplace culture can lead to:

- incentives that encourage fraudulent or corrupt behaviour
- 'win at all costs' attitudes that disregard risks or unethical behaviour
- tolerance for cutting corners or workarounds
- a culture where employees fear retaliation for raising process failures or ethical concerns
- bullying behaviour or employees being coerced to 'get on board with the programme'
- demoralised or resentful employees who may then rationalise fraudulent or corrupt actions.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- undertaking an employee survey that includes questions on workplace culture

- identifying unethical behaviours through discussion with employees
- identifying areas of improvement by completing quantitative and trend analysis of incidences of bullying and harassment, compensation, fraud and misconduct
- reviewing completion rates of relevant courses, e.g. ethics training
- checking whether employee turnover rates are a result of the organisation's culture.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Governance and oversight
- Help and support
- Integrity checks and suitability assessments
- Sufficient resourcing
- Trained and qualified employees

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The enabler
- The exploiter
- The organised

Governance and oversight

Establish governance and oversight mechanisms to oversee critical decisions and risks.

This control targets internal fraud risks.

Examples

Examples of this control include:

- programme or project reporting requirements and governance arrangements to ensure transparency and accountability
- executive boards and committees overseeing operations and making decisions
- defined accountabilities, responsibilities and reporting lines for programme or project performance and risk
- risk management plans and regular risk reporting
- assurance processes, e.g. pressure testing to assess the effectiveness of controls
- having processes in place to report internal and external framework and standards breaches
- frameworks that incentivise finding and reporting fraud or error.

Risks from control gap

A lack of good governance and oversight can:

- lead to dysfunctional and unclear processes
- cloud the visibility of fraud and corruption risks
- limit the ability to prevent, detect and respond to fraud and corruption
- enable employees or contractors to misuse their position of trust to commit fraud or corruption without being detected
- expose employees or contractors to coercion, where they may be pressured or intimidated into committing fraud for the benefit of another.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- reviewing governance structures to confirm that there are clear reporting lines and accountability for programme or project performance and risk
- confirming that executive oversight exists for critical processes and decision making
- confirming that risk management plans or fraud risk assessments have been completed, and that they are monitored and reported to appropriate managers
- confirming that identified fraud risks have an accountable person assigned to them
- identifying how governance structure requirements and responsibilities are communicated
- undertaking an employee survey that includes questions on reporting requirements and executive oversight
- performing comparative analysis against similar programmes and policies.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Activity reporting
- Defined decision-making powers
- Ethical culture
- Internal audits or reviews
- Policies
- Procedural instructions or guidance
- Public transparency
- Strategic partnerships

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The enabler
- The exploiter
- The organised

Help and support

Provide guidance and support to customers, employees and third parties to ensure they follow correct processes, comply with rules and meet expectations.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- clear statements about behaviour that is not acceptable
- clear guidance documentation outlining rules and eligibility criteria
- telephone support and coaching
- web content, chatbots and frequently asked questions
- regular communications on updates and requirements.

Risks from control gap

A lack of help and support for individuals to understand requirements and follow correct processes can lead to:

- frustrated employees, clients or third parties who may become motivated to commit fraud or rationalise fraudulent or corrupt behaviour
- clients, employees or third parties acting inconsistently or making errors resulting in higher levels of non-compliance
- weaknesses in processes and controls that fraudsters can exploit
- less visibility of fraud and corruption risks
- fraud or corrupt activity going unnoticed or unchallenged.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming help and support guidelines are documented, current and accessible
- conducting trend analysis of call wait times to identify whether delays in accessing support may increase non-compliance, workarounds or fraud risk

- walking through the programme to assess how easy it is for a user to understand requirements, access support and complete the process correctly
- undertaking testing or a process walkthrough to confirm that help and responsive support is provided in practice
- ensuring there are feedback and reporting processes in place to keep help and support guidelines relevant and identify opportunities for improvement
- undertaking an employee survey that includes questions on receiving coaching, communication and support.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Automatic prompts and alerts
- Escalation procedures
- Fraud awareness training
- Governance and oversight
- Procedural instructions or guidance
- Sufficient resourcing
- Trained and qualified employees

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The enabler
- The exploiter

Managerial or independent oversight

Involve more senior or independent personnel in actions, approvals and decisions to increase transparency and reduce the opportunity for fraud.

This control targets internal fraud risks.

Examples

Examples of this control include:

- a manager overseeing employee activities, e.g. work output, timesheets and travel
- a probity advisor reviewing and signing off procurement milestones
- a contract manager overseeing contract requirements, e.g. reporting on software development milestones
- a security advisor overseeing physical security arrangements.

Risks from control gap

Little or no managerial or independent oversight over employee actions and decisions can:

- lead to dysfunctional, inconsistent or obscure processes
- cloud transparency and visibility of fraud and corruption risks
- reduce accountability needed to prevent, detect and respond to fraud and corruption.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming the existence of processes to support transparent actions and decision making
- confirming that managerial or independent oversight exists for critical actions or decisions
- reviewing a sample of decisions to confirm managerial or independent advice was obtained

- reviewing workflows to ensure the involvement or oversight of a manager or independent person
- reviewing the workload to determine if oversight mechanisms can reasonably keep pace with the volume of actions and decisions
- reviewing reporting and reconciliation processes
- undertaking an employee survey that includes questions on the adequacy of supervisor oversight.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Defined decision-making powers
- Governance and oversight
- Internal audits or reviews
- Procedural instructions or guidance
- Sufficient resourcing

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The enabler
- The exploiter

Strategic partnerships

Promote sharing of information, capability and intelligence to prevent and disrupt fraud.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- partnerships with other government agencies, committees and taskforces to share information and data
- working with policy teams to contribute to programme design and implement legislative , policy and procedural changes
- collaborating with internal networks to share learnings and improve processes
- collaborating with international counterparts to share expertise and improve processes
- establishing or joining relevant communities of practice.

Risks from control gap

A lack of collaboration with strategic partners can lead to:

- less visibility of fraud and corruption risks, including cross-programme risks
- fraud or corrupt activity going unnoticed or unchallenged
- less action and accountability to prevent, detect and respond to fraud and corruption
- unknown and unaddressed systemic fraud and corruption.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- checking documentation and outcomes to ensure that regular collaboration is taking place
- reviewing the frequency of attendance and contributions to key meetings and forums

- reviewing the level of representation at key meetings and forums . Is this consistently delegated to subordinates?
- consulting stakeholders to understand their views on the agency's level and quality of engagement
- confirming existence of formal documentation, e.g. a memorandum of understanding.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Automatic data matching
- Coordinated disruption activity
- Fraud detection software
- Fraud investigation policy
- Governance and oversight
- Sufficient resourcing
- Watchlists

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The impersonator
- The organised

Sufficient resourcing

Have sufficient staffing and technical resources to enable processes, checks and oversight to function adequately.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- adequately staffing frontline services to properly collect and verify relevant information
- adequately staffing counter fraud and compliance areas to identify fraud vulnerabilities in programmes
- adequately resourcing fraud detection and response employees
- ensuring ICT systems have the functionality, security and capacity required to support counter fraud activities effectively.

Risks from control gap

Inadequately resourced prevention and compliance processes, checks and oversight can lead to:

- potentially suspicious matters not being dealt with
- frustrated employees, clients or third parties who may become motivated to commit fraud or rationalise fraudulent or corrupt behaviour
- employees making errors or applying processes inconsistently due to workload pressures, leading to higher levels of non-compliance and fraud
- employees not applying processes and controls correctly, such as identity authentication, which fraudsters can exploit
- employees not recognising inconsistencies or red flags, e.g. someone providing false or misleading information or evidence to support a request or claim
- poor management of fraud and corruption risks
- employees abusing their positions of trust to commit fraud or act corruptly.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- assessing the processing time for claims, registrations or other eligibility activities to ensure sufficient resourcing is in place
- monitoring performance activities to ensure adequate resourcing supports effective oversight
- conducting checks to see if processes are being followed properly
- undertaking a quantitative analysis of staffing levels and training completion
- analysing programme error rates and complaints
- checking that employee training plans and performance agreements clearly show the basic training they must complete
- undertaking an employee survey that includes questions on staffing levels.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Activity reporting
- Ethical culture
- Governance and oversight

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The enabler
- The organised

Trained and qualified employees

Provide employees with task-specific training to ensure that processes are followed and decisions are made correctly and consistently.

This control targets internal fraud risks.

Examples

Examples of this control include:

- all employees completing induction training on fraud prevention
- specific guidance, training and support to employees undertaking specialist processes
- all employees undertaking ethics and code of conduct training
- all employees completing mandatory qualifications and training to perform their duties.

Risks from control gap

Lack of adequate training for employees in how to apply correct processes and make appropriate decisions can lead to:

- frustrated employees, clients or third parties who may become motivated to commit fraud or rationalise fraudulent or corrupt behaviour
- employees acting in an inconsistent way or making errors resulting in higher levels of non-compliance and fraud
- employees not applying processes and controls correctly, e.g. identity authentication, which fraudsters can exploit
- employees not recognising inconsistencies or red flags, e.g. someone providing false or misleading information or evidence to support a request or claim
- poor management of fraud and corruption risks
- employees abusing their positions of trust to commit fraud or act corruptly.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- undertaking a quantitative analysis of staff training completion
- verifying that employees have the necessary qualifications to perform their duties
- analysing programme error rates and complaints
- asking employees about processes or systems to make sure they have received training
- checking that employee training plans and performance agreements clearly show the basic training they must complete
- undertaking an employee survey that includes questions on learning and development.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Defined decision-making powers
- Ethical culture
- Fraud awareness training
- Procedural instructions or guidance
- Quality assurance checks
- Specific and consistent processes

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The enabler
- The exploiter
- The impersonator

Prevention controls

Prevention controls are designed to proactively reduce the likelihood of fraud and corruption occurring by strengthening the organisation's control environment and minimising opportunities for misconduct. These controls focus on addressing the root causes of fraud risk, such as weak processes, unclear expectations or insufficient oversight.

A range of prevention controls can be implemented, and clear policies and procedures also play a critical role in setting expectations and guiding ethical behaviour across the organisation.

Prevention controls should be tailored to the organisation's specific fraud risk profile, operating environment and risk tolerance. This ensures that controls are proportionate, practical and targeted to higher-risk areas. Regular review and adjustment of these controls help maintain their effectiveness as risks evolve, supporting a proactive and resilient approach to fraud prevention.

Access controls

Limit access to systems, data, information, physical documents, offices and assets.

This control targets internal fraud risks.

Examples

Examples of this control include:

- login identification, biometrics and/or password requirements to access systems
- approving a request from employees before providing access to internal systems
- two-factor authentication to access an online account
- restricting access to different parts of a building
- restricting access to an online provider system to registered providers only
- ensuring employees can only access emails on work devices, not personal or public devices
- classified documents being stored in secure lockable cabinets.

Risks from control gap

Failing to implement effective access controls can lead to:

- employees or contractors accessing or manipulating systems and information without authority
- fraudulent payments, claims or requests being processed
- unauthorised access, use or disclosure of information or assets, leading to privacy or security breaches
- theft or misappropriation of monetary, data or physical assets for personal or third-party gain.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that controls comply with the Protective Security Requirements
- reviewing access control procedures to ensure employees know which rules apply in different situations and do not rely on judgement or workarounds
- confirming that requests for access processes are robust and that approvals are consistently applied
- confirming that only those who need access have been granted access
- reviewing processes that distinguish between requests from individuals who do not need access and those who do
- confirming that access is removed in a timely manner
- confirming that employees understand how to process access controls correctly and consistently
- confirming that employees cannot bypass process requirements, even when pressure or coercion is applied
- reviewing past access breaches to identify how they occurred and how they can be prevented in the future.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Automatic prompts and alerts
- Data protection
- Eligibility requirements
- Escalation procedures
- Identity verification
- Mandatory information
- Parameters and limits
- Record reconciliation
- Sensitive information access
- Sensitive information control
- User permissions

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The exploiter
- The impersonator

Accurate information collection

Collect accurate and relevant information to help process claims; make decisions; check, verify and analyse data; and investigate potential fraud.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- putting systems in place to independently check and verify the accuracy of data
- having clear and relevant categories of data to be collected that can be matched with relevant stakeholders
- having systems in place to confirm the identity of individuals providing data
- having clear, simple and secure processes for clients and stakeholders to update their data.

Risks from control gap

Providing services or funding to someone without collecting accurate and relevant data or information can lead to fraudsters:

- impersonating clients or third parties to receive fraudulent payments or gain access to information
- providing false or misleading information to support a request or claim
- using stolen identity documents to support a request or claim
- obtaining benefits or services they are not entitled to
- benefiting from incorrect decisions or payments.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- reviewing data collection controls and policies to see if they conform to national guidelines and frameworks, e.g. New Zealand data and information management principles and the Privacy Act 2020
- reviewing the rationale for information collection to confirm that data requirements are appropriate, proportionate and aligned with information available from authoritative public sources, e.g. New Zealand Companies Office
- confirming the existence of reference and guidance material
- confirming processes are consistently applied across all systems, platforms and communication methods
- reviewing a sample of completed transactions to confirm correct processes were undertaken
- asking employees about data collection to make sure they have a consistent and correct understanding
- undertaking control testing or a process walkthrough to confirm there is no way around processes
- identifying how the requirement to collect accurate and relevant data is communicated to employees
- identifying whether a lack of accurate or relevant data hinders claims or data matching
- reviewing identified cases of fraud involving exploitation of inaccurate data or a lack of relevant data.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Accurate information maintenance
- Automatic data matching
- Identity verification
- Information verification
- Mandatory information
- Procedural instructions or guidance
- Sufficient resourcing

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The enabler
- The exploiter
- The impersonator
- The organised

Accurate information maintenance

Create policies, rules, processes and systems that check, update and verify information and data where possible.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- regularly checking information with clients to ensure it is accurate and up to date
- flagging potentially old and outdated information
- matching information with more up-to-date records
- having processes to notify and confirm with clients when their information is updated
- having systems in place to independently check and verify the accuracy of data
- having systems in place to confirm the identity of individuals providing data
- requiring clients and stakeholders to update any changes in their circumstances
- having clear, simple and secure processes for clients and stakeholders to update their data
- having systems in place to identify and monitor changes to data
- having systems in place to secure and limit access to data.

Risks from control gap

Providing services to someone without having accurate data can lead to:

- fraudsters impersonating clients or third parties to receive fraudulent payments or gain access to information
- someone providing false or misleading information to support a request or claim
- fraudulent payments being made multiple times
- dual claiming of different payment or benefit types

- incorrect and inconsistent reporting and decision making
- other control weaknesses, e.g. less effective fraud detection.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that clear and consistent processes exist for checking, updating and correcting information and data
- analysing data to confirm incorrect information can be identified and corrected
- confirming the existence of reference and guidance material
- checking if and how incorrect information is reported
- identifying how the requirement to maintain accurate information and data is communicated to employees, clients and stakeholders
- identifying whether claims or data matching are hindered by not having accurate data
- surveying clients to check when and how they update information
- reviewing identified cases of fraud involving the exploitation of inaccurate data.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Accurate information collection
- Automatic data matching
- Data protection
- Information verification
- Mandatory information
- Specific and consistent processes

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The enabler
- The exploiter
- The fabricator

Approval workflows

Use system workflows to make sure all requests, claims or activities are approved only by the appropriate decision maker.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- a system automatically assigning requests to the correct decision maker for approval
- requiring all travel spending to be approved by the appropriate decision maker
- a system automatically assigning higher-value claims to a specified approver, e.g. a central delegate
- the finance system automatically assigning purchase orders to the procurement team and spending approvers.

Risks from control gap

Allowing requests, claims or activities to be approved by someone other than the appropriate decision maker can lead to:

- employees processing fraudulent requests or claims for themselves or another person
- employee entitlements, e.g. leave or overtime, being approved without the knowledge or approval of the manager or delegate
- processes becoming uncertain or not working properly
- poor management of decision making and risk.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming the existence of approval workflows within the system
- consulting employees about approval processes to confirm they have a correct understanding

- identifying how approval requirements are communicated to employees
- reviewing procedures or guidance to confirm they clearly specify approval processes
- reviewing requirements on how approvals are obtained
- confirming approval processes are consistently applied
- confirming that someone cannot override or bypass approval processes, even when pressure or coercion is applied
- reviewing a sample of completed requests or claims to confirm appropriate approval was obtained on all occasions
- reviewing reports of completed requests, claims or activities to confirm approval is obtained on all occasions
- undertaking fraud control testing or a process walkthrough to confirm that approval processes are enforced
- confirming the existence of a review and reconciliation process and reviewing the reports
- reviewing any past fraud cases to identify how they were allowed to occur.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Access controls
- Defined decision-making powers
- Escalation procedures
- Privileged system access
- Sensitive information access
- User permissions

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The enabler
- The exploiter

Automatic prompts and alerts

Set up system prompts and alerts to warn users when information is inconsistent or irregular.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- informing users or claimants upfront about their obligations
- alerting users when transactions do not comply with policy, e.g. when the cheapest available fare is not selected
- requiring an applicant to provide correct information in an online form, e.g. alerting a user when an applicant mistakenly enters a future date for their date of birth
- requiring employees or applicants to confirm the accuracy of information provided.

Risks from control gap

A lack of automatic prompts and alerts can lead to:

- fraudsters feeling more confident that their actions will not be detected
- individuals deliberately or accidentally not disclosing information that could affect entitlements
- individuals deliberately or accidentally providing false information or evidence to support a request or claim
- fraudulent activity being carried out using an individual's account or identity without their knowledge
- increased opportunities for omissions and errors.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- checking that prompts and alerts are easy for users to understand

- confirming that prompts and alerts are consistent across systems
- confirming that prompts and alerts are implemented correctly by doing pressure testing or a process walkthrough
- confirming if claims still contain errors despite the prompts and alerts that exist
- measuring behaviour before and after the implementation of prompts and alerts
- confirming that the number of requests with errors has decreased after prompts and alerts have been implemented
- confirming that employees have received prompts or alerts and know what to do in response
- consulting with behavioural insights experts to see if they identified a change in behaviour after prompts and alerts were implemented.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Data protection
- Eligibility requirements
- Mandatory information
- Parameters and limits
- Privileged system access
- Specific and consistent processes

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The exploiter
- The impersonator

Change management processes

Implement change management processes to ensure changes do not create vulnerabilities or weaken existing fraud controls.

This control targets internal and external fraud risks.

Examples

Examples of this control include:

- engaging with employees and/or clients before, during and after changes are implemented
- undertaking and updating fraud risk assessments when there is a substantial change in the structure, functions or activities of the organisation or programme
- making sure changes go through a rigorous and transparent change management process
- consulting fraud control teams about programme and system changes
- undergoing a change impact assessment to consider the potential impacts on existing fraud controls when major changes occur
- logging all system changes through a change management system
- controlling all updates to access controls and source codes through layers of security, such as biometrics and transaction monitoring.

Risks from control gap

Changes to systems outside a transparent change management process can lead to:

- new or increased fraud and corruption risks
- unintended removal of existing controls
- vulnerabilities in existing controls
- employees and contractors being coerced to commit fraud for the benefit of another person or organisation
- fraudsters hiding changes in systems to create loopholes or defects to:
  - facilitate fraudulent payments
  - access, manipulate or release sensitive information
  - erase records of their activities.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- undertaking a desktop review of change management policies and processes to confirm that clear and consistent processes exist
- confirming that change management processes align with existing policies
- confirming that change impact assessments and risk plans are completed and reviewing the documentation
- confirming that risk plans are used and updated
- consulting subject matter experts on change processes to evaluate their understanding and thoughts about fraud risk
- confirming that change processes would effectively identify and manage fraud risks
- confirming that fraud control teams are engaged as a stakeholder during change processes
- confirming that risks are properly treated
- reviewing how changes are reported, e.g. ask if change management plans are reviewed and signed off by a project board
- confirming that post-implementation reviews occur
- undertaking an employee survey and including questions relevant to change management.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Governance and oversight
- Internal audits or reviews
- Procedural instructions or guidance
- Quality assurance checks
- Sufficient resourcing

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The enabler
- The exploiter
- The organised

Compliance, performance and contract reviews

Require clients, employees and third parties to have ongoing compliance, performance and contract reviews.

This control targets internal fraud risks.

Examples

Examples of this control include:

- undertaking regular compliance checks with providers and clients
- reassessing the suitability of service providers, contractors or vendors
- only allowing clients to continue to receive payments if they meet certain ongoing requirements
- regularly reviewing and monitoring employee performance
- regularly reviewing contract performance to make sure requirements are being met.

Risks from control gap

A lack of ongoing compliance, performance and contract reviews can lead to:

- acting dishonestly or without care once a benefit, grant or contract has been awarded
- providing false information about their ongoing work performance or the delivery of contract obligations
- failing to disclose changes in circumstances that might affect their ongoing entitlement to a benefit or payment
- failing to disclose changes that may affect their ability to meet contract conditions
- retaining access to systems or information when it is no longer required.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- analysing completed reviews to confirm these are undertaken regularly or as required
- reviewing a sample of completed requests or claims to confirm reviews are undertaken with appropriate attention to detail
- reviewing procedures or guidance to confirm they clearly specify how reviews are to be undertaken
- confirming reviews are consistently undertaken
- asking employees about the review processes or systems to make sure they have a correct understanding
- analysing statistics and reports on employee performance reviews
- identifying how ongoing compliance, performance and contract requirements are communicated to employees, customers and third parties
- confirming that someone cannot bypass review requirements, even when under pressure or coercion.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Accurate information collection
- Automatic data matching
- Contractual clauses
- Eligibility requirements
- Specific and consistent processes

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The enabler

Contractual clauses

Develop contractual clauses to help prevent, detect and respond to fraud or non-compliance.

This control targets both internal and external fraud risks.

Examples

Examples of this control include contractual clauses that:

- set out requirements to report fraud
- set out requirements to have counter fraud arrangements in place
- define obligations and/or permissions
- set out liability for fraud and clawback arrangements
- allow access to premises and documents for quality assurance, compliance and investigation purposes
- obtain consent to collect and share information
- require directions to be followed in the event of suspected fraud
- allow recovery of debts and fraud losses
- are easy to comply with.

Risks from control gap

A lack of clear contractual clauses can lead to:

- fraudsters deceiving others to take advantage of loose rules and unclear processes to commit fraud and avoid exposure or prosecution
- limiting an organisation's ability to take effective legal or counter fraud action
- inability to recover funds in the event of fraud occurring.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming contractual clauses are clear, fit for purpose and legally enforceable, in line with the organisation's activities and applicable legislation

- confirming that employees can easily find and reference contractual clauses
- confirming that employees can easily understand and apply contractual clauses
- asking employees about any known vulnerabilities in contracts that may increase rates of non-compliance or fraud
- asking employees about any contractual clauses that limit their ability to collect, use and disclose information to prevent, detect and respond to fraud
- asking employees about any contractual barriers to conducting fraud investigations, enforcing penalties and recovering fraud losses.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Compliance, performance or contract reviews
- Defined decision-making powers
- Governance and oversight
- Penalties for fraud or non-compliance
- Procedural instructions or guidance

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The exploiter
- The fabricator

Counter fraud messaging

Use strong counter fraud messaging to encourage would-be fraudsters to think twice before committing fraud and explain how people should respond to suspicious activity in the workplace.

This control targets both internal and external fraud risks.

Examples

Examples of this control include making statements that:

- most people do the right thing; they behave honestly and support the community by reporting suspected fraud
- reduce the perceived benefits of fraud by showing fraudsters they are likely to be caught and identified
- evoke an emotional reaction (e.g. fear, guilt or empathy) and appeal to a person's desire to do the right thing
- highlight your organisation's commitment to disrupting fraud and protecting the integrity of its systems.

Risks from control gap

A lack of clear, effective counter fraud messaging can lead to:

- individuals underestimating the likelihood that fraudulent behaviour will be detected
- people perceiving fraud as low risk and high reward
- individuals believing that consequences will be minimal or unlikely
- fraudsters exploiting perceived gaps in monitoring and enforcement
- potential fraudsters not fearing any consequences.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- analysing data to identify changes to behaviour before and after communications have been made

- reviewing when deterrence messages are delivered. Do they prompt people when they are likely to be most receptive? E.g. when a claim is initiated, when approval is sought, or for any other notifiable events and changes that impact ongoing eligibility
- confirming deterrence messages are obvious and attract attention
- reviewing the design of claim or application forms to ensure deterrence messages are placed upfront
- reviewing deterrence messages to ensure information is presented in plain and direct language
- confirming forms use simple and binary questions to make it more difficult for a person to rationalise providing false or misleading information.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Help and support
- Procedural instructions or guidance
- Public transparency
- Strategic partnerships

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The enabler
- The exploiter

Data protection

Protect data from being manipulated or misused.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- securing prefilled data on forms so that it cannot be changed
- securing reports as read-only to prevent manipulation
- ensuring that data coded directly into systems cannot be manually altered
- restricting updates to production data by restricting a system's parameters
- restricting alterations to a system's source code outside a prescribed change management process
- restricting changes to audit logs
- ensuring requirements under the Protective Security Requirements are adhered to
- ensuring that original copies of data are recorded and stored separately.

Risks from control gap

Allowing data within systems or prefilled forms to be manipulated by clients, employees or third parties could allow fraudsters to:

- submit false claims using manipulated information or evidence
- conceal or erase information or evidence
- facilitate fraudulent payments
- update information without authority
- improperly influence decisions using false or manipulated information.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- reviewing procedures or guidance to confirm it clearly specifies how data should be protected from manipulation or misuse
- reviewing controls and policies to see if they conform with the Protective Security Requirements
- confirming protections are in place to prevent data being manipulated or misused
- confirming protections are always applied by employees
- confirming that appropriate protections and classifications are being applied by reviewing a sample of completed data requests
- confirming that data has not been manipulated by doing quantitative analysis, e.g. reconciling audit logs
- confirming that data has not been manipulated by reviewing a sample of data
- confirming that data cannot be manipulated by doing pressure testing or a process walkthrough.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Access controls
- Audit logging
- Automatic data matching
- Privileged system access
- Sensitive information access
- User permissions

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The enabler
- The fabricator

Declarations

Use declarations to communicate and confirm that a person understands their obligations and the consequences of non-compliance.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- requiring applicants to complete a declaration when submitting a claim or request, e.g. "I declare the information provided is true and correct and I acknowledge the consequences for providing false or misleading information"
- requiring employees to sign a declaration or acknowledgement confirming they have read and understood privacy and information access policies
- obtaining consent from employees, funding recipients , contractors or providers for their personal information (including banking information) to be shared to prevent, detect or investigate fraud
- obtaining consent from contractors or providers to give access to premises or records to investigate fraud.

Risks from control gap

Not requiring declarations can lead to:

- applicants providing false information or misleading statements to support a request or claim
- applicants concealing or withholding information that would affect their entitlement.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming declarations exist on relevant forms
- confirming that the consequences of non-compliance are clearly communicated

- confirming the completion of a declaration is mandatory and/or may have legal effect
- reviewing the content and wording to make sure it clearly encourages compliance and deters fraud
- checking where and how records of completed declarations or acknowledgements are kept
- consulting behavioural insights experts about the declarations and acknowledgements
- asking employees about their understanding of the declaration and the consequences for non-compliance.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Eligibility requirements
- Mandatory information
- Penalties for fraud and non-compliance
- Specific and consistent processes
- Trained and qualified employees

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The enabler
- The fabricator

Decommissioning and disposal

Have processes in place to properly archive or dispose of old or unnecessary information and communications technology (ICT) systems, assets, documents and records.

This control is supported by the Protective Security Requirements and the information and records management standard under the Public Records Act 2005.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- archiving information or ceasing a client identity
- disposing of documents in accordance with the relevant records authority
- making sure expired building passes are surrendered to the issuing authority
- regularly reviewing vacant human resources position numbers and removing them if no longer required
- appropriately handling and destroying returned unclaimed mail
- effectively disposing of redundant ICT stock
- withdrawing access to ICT systems and resources when employees leave
- withdrawing privileged access to ICT systems when no longer required
- protecting deceased client records from misuse, e.g. by making them read-only
- protecting redundant provider or supplier accounts from misuse, e.g. by making them read-only
- checking physical assets, e.g. safes and furniture, before disposal.

Risks from control gap

Keeping old or unnecessary ICT systems, employee position numbers and access, controls, client accounts, assets or records may allow fraudsters to:

- use old human resources position numbers to make fraudulent payroll payments
- receive payments for deceased customers
- impersonate public officials
- steal surplus assets
- access, exploit and/or release information held in old or unused systems or hardware
- access, exploit and/or release information held in old physical storage
- use stolen records to make fraudulent requests or claims.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- reviewing policies and processes to confirm that clear and consistent processes exist
- consulting subject matter experts on processes and systems to evaluate their understanding and thoughts about fraud control policies
- conducting a process walkthrough by having employees show you the archive or disposal process
- reviewing who has access to perform archive or disposal processes
- testing and confirming that archived records cannot be manipulated
- analysing data or reports to confirm old or unnecessary systems, employee positions and accesses, client accounts, assets or records are being properly archived or disposed of
- reviewing a data sample to confirm compliance with policies and processes
- checking if and how archive or disposal processes are reported.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Change management processes
- Governance and oversight
- Procedural instructions or guidance
- Specific and consistent processes
- Trained and qualified employees

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The exploiter
- The fabricator

Disclosure and reporting

Require and support employees and third parties to disclose gifts, benefits, incidents, mistakes, and real or perceived conflicts of interest.

This control targets internal fraud risks.

Examples

Examples of this control include:

- requiring employees to declare conflicts of interest
- requiring employees to report gifts, benefits and hospitality
- creating a process for employees to report accidental unauthorised accesses or disclosures
- requiring employees or contractors to report when their circumstances change, e.g. to maintain a security clearance.

Risks from control gap

Lack of disclosure and reporting processes can lead to or disguise:

- employees and third parties failing to disclose gifts, benefits, incidents, mistakes and real or perceived conflicts of interest
- fraudulent conduct, dishonest influence or corruption
- employees and contractors being coerced to commit fraud for the benefit of another person or organisation.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming policy and guidance material exists for disclosure or reporting
- confirming guidance material is available and easy to access
- reviewing guidance material to make sure it is clear and easy to understand
- confirming that registers for reporting exist and are easily accessible

- asking employees about the disclosure forms, processes or systems to make sure they have a consistent understanding of how to use them
- analysing the use of registers, e.g. for gifts, conflicts of interest, or incidents and mistakes.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Avenues for reporting fraud
- Ethical culture
- Fraud awareness training
- Governance and oversight
- Procedural instructions or guidance

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The enabler
- The fabricator

Duplicate prevention

Put processes in place to prevent, identify and correct duplicate records, identities, requests or claims.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- identifying and denying duplicate claims
- flagging and reviewing potential duplicate vendor invoices
- requiring employees to undertake thorough searches of existing customer records to avoid creating duplicate records
- interrogating systems to identify, review and correct potential duplicate records.

Risks from control gap

Duplicate records, identities, requests or claims can lead to:

- fraudulent payments being made multiple times
- dual claiming of different payments or benefit types
- duplicate or ghost records being used to conceal activities or exploit processes
- incorrect and inconsistent reporting and decision making
- other control weaknesses, e.g. less-effective fraud detection.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that clear and consistent processes exist to prevent, identify and correct duplicates
- analysing data to confirm duplicates are being properly identified and corrected
- consulting subject matter experts on processes
- conducting a system or process walkthrough by having employees show you the process for managing duplicates

- reviewing a data sample to confirm compliance with policies and processes
- reviewing who has access to review and correct duplicates
- checking if and how duplicates are reported.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Automatic data matching
- Identity verification
- Information verification
- Procedural instructions or guidance
- Specific and consistent processes

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The enabler
- The exploiter
- The fabricator
- The impersonator

Eligibility requirements

Have clear and specific eligibility requirements and only approve requests or claims that meet the criteria.

This control targets internal fraud risks.

Examples

Examples of this control include:

- income tests or requirements, e.g. a claimant's taxable income or business turnover must be below $100,000
- age requirements, e.g. programme recipients must be over the age of 67 years
- residency requirements, e.g. programme payments are only available to New Zealand residents
- geographical requirements, e.g. programme recipients must reside in a particular location
- qualification requirements, e.g. potential vendors must possess appropriate licences
- preconditions, e.g. employees cannot be issued with a building pass prior to the completion of an entry-level check
- expenditure requirements, e.g. expenditure on a project must be above/below $100,000
- quantitative requirements, e.g. claimants can only claim for a certain number of hours or people
- eligibility requirements to fast track or provide additional scrutiny for claims, e.g. a family claiming for more than five children is required to undergo additional checks.

Risks from control gap

Failing to specify clear eligibility requirements or verify a person's eligibility for a request or claim can lead to:

- fraudsters exploiting weaknesses to receive payments or services they are not entitled to
- fraudsters accessing information or systems without a business need

- fraudsters providing false information or evidence to support a request or claim
- fraudsters hiding information that would affect their entitlement
- reduced ability to adequately investigate and respond to fraud and corruption.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- reviewing a sample of completed requests or claims to confirm that correct eligibility determinations are being made
- reviewing approval processes to see if there is a segregation of duties
- calculating how many reviews result in a reversal of the original eligibility decision
- confirming that employees receive training about eligibility requirements
- confirming that employees have access to reference materials that set out required standards for eligibility requirements
- confirming that employees understand what the eligibility criteria are and how to apply them consistently
- undertaking testing or a process walkthrough to confirm that eligibility determinations cannot be manipulated or bypassed, even when pressure or coercion is applied.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Duplicate prevention
- Identity verification
- Information verification
- Mandatory information
- Specific and consistent processes

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The enabler
- The exploiter

Employee and contractor rotation

Rotate employees and contractors to reduce over-familiarity with systems and limit opportunities for malicious activity.

This control targets internal fraud risks.

Examples

Examples of this control include:

- regularly rotating employees in high-risk positions
- rotating contract managers so they do not develop a conflict of interest with suppliers.

Risks from control gap

Leaving employees and contractors in positions for too long can lead to:

- less visibility of fraud and corruption risks
- employees or contractors taking advantage of positions of trust to act corruptly, commit fraud and avoid exposure
- employees and contractors becoming overly familiar with processes and learning how to exploit weaknesses
- fraud or corruption going undetected for a long period of time
- employees being targeted and coerced to process fraudulent claims or invoices for another person or organisation.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming the existence of a rotation policy or best practice guidelines for rotating employees through high-risk roles
- confirming that high-risk roles are reviewed regularly
- reviewing procedures or guidance to make sure it clearly specifies requirements for rotation and contractor engagement
- reviewing statistics or reports on employees and contractor positions and durations.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Fraud awareness training
- Governance and oversight
- Integrity checks and suitability assessments
- Managerial or independent oversight
- Separation and termination processes
- Trained and qualified employees

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The enabler
- The exploiter
- The organised

Escalation procedures

Escalate non-standard requests or claims for further review or scrutiny.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- having an escalation point, e.g. a policy team or helpdesk , for more complex requests or claims
- escalating claims that exceed a certain monetary threshold for further scrutiny
- having a separate policy team review and action complex, uncommon or late claims.

Risks from control gap

A lack of internal processes to escalate non-standard requests or claims can lead to:

- disorganised or inconsistent practices and decision making
- fraudsters using confusion and deception to exploit processes
- fraudsters receiving payments or services they are not entitled to
- fraudsters accessing information or systems without a business need
- fraudsters providing false or misleading information or evidence to support a request or claim
- fraudsters concealing information that would affect their entitlement.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- reviewing the policies and procedures for escalating requests or claims
- confirming non-standard requests and claims are escalated to someone with sufficient delegation, independence or expertise

- confirming escalation processes are consistently applied
- analysing statistics of non-standard requests or claims to discover what percentage of claims fall in this category and if it aligns with the number of escalations
- reviewing a sample of non-standard requests or claims to confirm correct escalation processes were followed
- asking employees about internal escalation processes to make sure they have a consistent and correct understanding
- identifying how escalation requirements are communicated to employees
- confirming that someone cannot bypass escalation processes or systems, even when subject to pressure or coercion
- reviewing the training employees receive to make sure it includes information about escalation procedures.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Procedural instructions or guidance
- Specific and consistent processes
- Sufficient resourcing
- Trained and qualified employees

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The enabler
- The exploiter
- The fabricator

Fraud awareness training

Train and support employees to identify red flags so they know how to detect and report any suspected fraud.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- completing fraud awareness training as part of employee induction
- completing fraud awareness training for all staff every 12 months
- running fraud awareness campaigns
- having leadership send out strong and consistent messages about ethical organisational culture and fraud awareness
- providing clear and accessible fraud awareness content on the staff intranet
- having targeted training that is relevant to specific roles
- educating providers or grant recipients on what fraud is.

Risks from control gap

Employees who are not trained to identify and report fraud or corruption can lead to:

- dysfunctional workplace cultures
- fraudulent or corrupt activity going unnoticed or unchallenged
- fraudsters feeling more confident that their actions will not be identified and reported
- less action and accountability for preventing, detecting and responding to fraud and corruption
- unknown and unaddressed systemic fraud or corruption.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- reviewing training materials to determine if messages about fraud-related policies are clear and relevant to employees

- determining if training or reinforcement messages are regularly provided as planned
- conducting interviews, workshops or surveys with employees to ensure that they understand fraud-related policies
- creating case studies showing situations where employees who have completed fraud awareness training have subsequently gone on to report fraud or proactively fix vulnerabilities
- checking that employees can easily access training and other support materials
- undertaking an employee survey that includes questions about understanding fraud risk and corruption, and how to report it
- confirming that there is regular fraud awareness training scheduled for all staff.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Avenues for reporting fraud
- Ethical culture
- Governance and oversight
- Help and support

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The exploiter
- The fabricator
- The impersonator
- The organised

Identity verification

Authenticate client or third-party identities during each interaction by testing the credentials supplied by the person making the claim.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- using RealMe to confirm an individual's identity online
- performing entry-level checks to confirm the identity of employees and contractors
- requiring service providers to present evidence of identity for company directors
- requiring applicants to provide certified copies of primary and secondary identification.

Risks from control gap

Accepting claims or requests without confirming an applicant's identity can lead to:

- fraudsters impersonating customers or third parties to receive fraudulent payments or gain access to information
- fraudsters using false or stolen identities to receive fraudulent payments or gain access to information
- spoofing, which is the act of disguising communication from an unknown source as being from a known, trusted source.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- reviewing identity verification policies to make sure it is clear when a policy applies
- reviewing a sample of completed claims to confirm correct processes are being carried out

- reviewing identified cases of fraud that used a false or stolen identity to confirm whether changes are required to identity verification processes
- confirming that employees are applying processes consistently both within and across channels.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Automatic data matching
- Information verification
- Mandatory information
- Procedural instructions or guidance
- Sensitive information control
- Sufficient resourcing

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The enabler
- The exploiter
- The organised

Integrity checks and suitability assessments

Assess and confirm the integrity and suitability of new employees, contractors or third parties.

This control targets internal fraud risks.

Examples

Examples of this control include:

- pre-employment checks, e.g. criminal record and credit checks for all new employees, contractors or third parties
- robust reference checking processes
- trial periods for all new employees, contractors or third parties
- requiring all employees, including contractors, to have and maintain the appropriate security clearance for designated roles, in accordance with the Protective Security Requirements
- ongoing checks after onboarding employees or clients
- verifying that businesses have a valid New Zealand Business Number and confirming their details, e.g. by searching the Companies Register website.
- checks in accordance with the Protective Security Requirements.

Risks from control gap

Ineffective integrity checks and suitability assessments can lead to:

- organisations hiring employees, contractors or third parties who lack integrity and go on to create insider threats or contribute to a dysfunctional organisational culture
- costly frauds and reputational damage
- employees, contractors or third parties abusing their position of trust to commit fraud or act corruptly
- employees, contractors or third parties being coerced to commit fraud for the benefit of another person or organisation.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- reviewing the integrity checks process for new employees, contractors, vendors or providers
- reviewing the process for ongoing suitability assessments throughout the employment or engagement period of employees, contractors or third parties
- reviewing suitability assessment processes to confirm that they align with the Protective Security Requirements
- identifying whether there is a high number of contracts that are terminated during or after an initial trial period, which may indicate that the initial screening process or suitability assessment is not operating effectively
- analysing data from integrity checks and suitability assessments and confirming that these are always completed
- undertaking an employee survey that includes questions on awareness of integrity issues and how to report them
- identifying positions that require a security clearance and confirming that each employee has the required clearance.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Accurate information collection
- Automatic data matching
- Compliance, performance and contract reviews
- Coordinated disruption activity
- Eligibility requirements
- Governance and oversight
- Identity verification
- Information verification
- Mandatory information
- Procedural instructions or guidance
- Separation and termination processes

- Specific and consistent processes
- Strategic partnerships
- Watchlists

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The organised

Mandatory information

Require mandatory information to be collected to support claims or requests.

This control targets external fraud risks.

Examples

Examples of this control include:

- mandatory fields to be completed for online claim forms
- applicants providing income and asset statements with their claim
- vendors providing business details, e.g. their New Zealand Business Number
- service providers, grant recipients or vendors to provide business details, e.g. their New Zealand Business Number, business address, email address, phone number, authorised contact and associates
- requiring supporting evidence to be submitted with claims.

Risks from control gap

Not collecting mandatory information to support claims or requests can lead to:

- manual follow-up and processing increasing the opportunities for omissions and errors
- fraudsters deliberately making false claims by omitting relevant information
- fraudsters receiving payments or services they are not entitled to
- fraudsters concealing information that would affect their entitlement to funding or services.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming the existence of reference and guidance material that clearly outlines what information is required

- confirming mandatory information is consistently obtained
- reviewing a sample of completed requests or transactions to confirm all mandatory information was provided
- asking employees about the mandatory requirements to make sure they have a consistent and correct understanding
- undertaking fraud control testing or a process walkthrough to confirm that mandatory information must be provided, even when pressure or coercion is applied
- identifying how mandatory requirements are communicated to employees, clients and third parties
- reviewing the training employees receive to make sure it includes information about collecting and using mandatory information
- reviewing approvals processes and make sure mandatory information is checked.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Eligibility requirements
- Identity verification
- Information verification
- Specific and consistent processes

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The fabricator
- The impersonator
- The organised

Parameters and limits

Apply parameters or limits to requests, claims or processes and enforce these limits using system controls.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- setting transaction limits for credit cards
- enforcing claim limits for programme payments
- restricting particular items or payments that can be claimed together
- only allowing customers, clients or registered nominees to make changes to bank accounts
- restricting payments for programmes so that they are made to New Zealand bank accounts only
- requiring the use of approved providers or vendors only.

Risks from control gap

Not having clear parameters to keep requests, claims or processes within set boundaries can lead to:

- disorganised, inconsistent practices and decision making
- fraudsters exploiting dysfunctional processes to receive payments or services they are not entitled to
- fraudsters receiving payments that are larger than they otherwise would get.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that employees understand and know how to use parameters and limits correctly and consistently
- reviewing a sample of completed requests or claims to confirm that parameters and limits are being applied effectively

- confirming that parameters and limits are used by doing pressure testing or a process walkthrough
- confirming that individuals cannot override or bypass parameters and limits, even when pressure or coercion is applied
- confirming that reporting or reconciliation processes exist and that claims or requests are within limits .

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Automatic prompts and alerts
- Procedural instructions or guidance
- Specific and consistent processes

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The enabler
- The exploiter
- The fabricator

Policies

Establish, maintain and communicate clear, enforceable and accessible policies that set expectations for lawful, ethical and transparent behaviour across the organisation.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- clear, up-to-date fraud, corruption and integrity policies
- policies governing conflicts of interest, gifts and benefits, hospitality and secondary employment
- clear procurement, contract management and supplier-related policies
- information security, privacy and data handling policies
- user access, system use and cybersecurity policies.

Risks from control gap

Poorly designed or poorly communicated policies can lead to:

- gaps that create opportunities for fraud, corruption or unethical conduct
- inconsistent decision making or unchecked discretionary authority
- employees misunderstanding what is acceptable or prohibited
- individuals exploiting ambiguity to rationalise fraudulent behaviour
- fraudsters taking advantage of loose rules and requirements to commit fraud and avoid exposure or prosecution
- less action and accountability to prevent, detect and respond to fraud and corruption.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- checking whether policies are current, accessible and aligned to legislative and organisational requirements

- analysing completion rates for mandatory training modules linked to key policies
- checking whether employees understand policies through surveys
- monitoring the number and nature of incidents arising from policy breaches
- analysing fraud trends to identify policy gaps.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Ethical culture
- Governance and oversight
- Integrity checks and suitability assessments
- Internal audits or reviews
- Trained and qualified employees

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The enabler
- The exploiter
- The organised

Privileged system access

Limit and monitor privileged system access that allows employees, contractors and providers to perform special functions or override system and application controls.

This control targets internal fraud risks.

Examples

Examples of this control include:

- only assigning privileged roles or accounts to employees who have an appropriate level of authority or security clearance
- only granting privileged system access on a temporary or as-needed basis
- regularly reviewing access to privileged roles and accounts
- increasing monitoring of employees with privileged system access, e.g. administrative access
- audit logging and regularly reporting on the use of privileged accounts
- adhering to requirements under the:
  - Protective Security Requirements
  - New Zealand Information Security Manual
  - Minimum Cyber Security Standards
  - NCSC Cyber Security Framework.

Risks from control gap

A lack of tightly restricted and monitored access can lead to:

- fraudsters gaining access and using it to conceal their activities or expand their access across systems
- uncertainty around how employees are using administrative privileges
- poor management of decision making and risk related to administrative privileges
- employees or contractors abusing their position of trust to process fraudulent requests or claims for themselves or another person

- employees or contractors abusing their position of trust to access and disclose official information without authority
- employees or contractors being coerced by others to use their administrative privileges for dishonest purposes
- employees or contractors using privileged access to make unauthorised changes to systems or databases to:
  - bypass approvals
  - access, manipulate or release sensitive information
  - erase records of their activities.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming controls comply with the Protective Security Requirements
- confirming the use of privileged accounts is controlled and auditable
- obtaining and reviewing requirements for who should have access to privileged accounts
- confirming the existence of a request and approvals process for obtaining privileged accounts
- confirming that someone cannot bypass standard process requirements, even when subject to pressure or coercion
- confirming that privileged accounts are subject to segregation of duties requirements
- reviewing the need for security clearances for privileged accounts
- reviewing a sample of circumstances where privileged accounts were used
- reviewing reports to confirm privileged accounts are only assigned to employees that require them
- undertaking testing or a process walkthrough to confirm that the limits and monitoring of privileged accounts work correctly and cannot be circumvented
- confirming that the use of accounts are reviewed and reconciled and checking the reports
- reviewing any past breaches or fraud related to the use of privileged accounts and identifying how they occurred.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Access controls
- Fraud awareness training
- Fraud detection software
- Internal audits or reviews
- Separation and termination processes
- User permissions

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The enabler
- The exploiter

Procedural instructions or guidance

Provide clear, documented processes and guidance related to activities or processes to employees.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- programme procedures and processes, or instructions for internal functions, e.g. credit card acquittals
- instructions for collecting the right information, e.g. to verify eligibility or entitlements
- procedures to help employees apply processes consistently and correctly
- guidance to help employees make correct and ethical decisions
- clear instructions for third parties to follow when completing applications.

Risks from control gap

A lack of clear guidance and procedural instructions can lead to:

- dysfunctional and obscure processes
- poor management of fraud and corruption risks
- a culture where incorrect processes and workarounds become the norm
- fraudsters taking advantage of loose rules and processes to commit fraud and avoid exposure or prosecution.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that procedural instructions or guidance materials exist
- confirming that employees can easily find and reference procedural instructions and guidance materials

- confirming that employees understand procedural instructions and guidance materials and use them
- confirming procedural instructions and guidance materials are regularly reviewed and updated
- reviewing access records of procedural instructions and guidance material to confirm employees are using it.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Defined decision-making powers
- Governance and oversight
- Internal audits or reviews
- Specific and consistent processes
- Trained and qualified employees

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The enabler
- The exploiter

Public transparency

Publish information on your organisation's decision-making processes, decisions made, successful tenderers or grantees, incidents and breaches.

This control targets both internal and external fraud risks.

Examples

Examples of this control include publishing information on:

- your organisation's decision-making processes
- organisations or individuals receiving government funding
- which decisions have been made
- approved providers or licence holders
- conflicts of interest from external influences
- fraud incidents.

Risks from control gap

Opaque decision-making processes, tenders and incidents can lead to:

- fraudsters concealing their corrupt or fraudulent activities
- inconsistencies in tender, grant or licensing processes
- repeat offending by fraudsters across organisations
- employees manipulating bidding criteria to favour a particular supplier.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- reviewing decision-making procedures
- reviewing information published on decisions
- interviewing employees and stakeholders to identify their awareness of decisions made
- confirming the existence of reference and guidance material to help in decision making

- reviewing conflict of interest registers
- reviewing how fraud incidents are reported and communicated.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Activity reporting
- Approval workflows
- Defined decision-making powers
- Governance and oversight
- Trained and qualified employees

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The exploiter
- The organised

Random allocation

Randomly allocate requests or claims to employees to remove the option for employees to select which claims to process.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- automatic push allocation in case management systems
- workflow-driven blind allocation where employees must take the oldest task in the queue first
- automating email or chat distribution rather than employees selecting emails from a shared inbox
- supervisors reviewing and assigning tasks via a team meeting or in a shared tracker.

Risks from control gap

Allowing employees to choose which requests or claims to process can lead to:

- employees deliberately processing fraudulent requests or claims
- employees being coerced to process fraudulent requests or claims by others.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming random allocation processes are always applied
- reviewing workload management specifications and system requirements
- reviewing reports of work allocation, e.g. by location and user identification
- undertaking fraud control testing or a process walkthrough to confirm that allocation processes cannot be circumvented, even when pressure or coercion is applied

- reviewing approvals processes and making sure there is a segregation of duties
- confirming monitoring and reporting processes exist for allocation and confirming this would identify abnormal processing patterns.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Procedural instructions or guidance
- Specific and consistent processes
- Sufficient resourcing
- User permissions

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The exploiter
- The organised

Segregation of duties

Share tasks and permissions for a specific business process among multiple employees.

This control targets internal fraud.

Examples

Examples of this control include:

- employees who can create and maintain vendor records cannot also process invoices
- the same employee cannot make, approve and reconcile credit card payments
- multiple employees must be involved in approving and processing grant payments
- employees who ordered assets from suppliers cannot confirm the delivery of the assets in the accounting system
- the same employee cannot record payroll information in the system and verify the calculation.

Risks from control gap

Allowing a single individual to complete multiple functions that should be segregated can lead to:

- fraudulent payments
- unauthorised access, manipulation or disclosure of information
- poor management of decision making and risks
- the creation of fake vendors
- fraudsters concealing their activities
- employees falling prey to spoofing, which is the act of disguising communication from an unknown source as being from a known, trusted source.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- consulting employees or subject matter experts about segregation of duties processes
- confirming employees have a correct understanding of the purpose of segregation of duties
- confirming that segregation of duties is enforced within the system where required
- confirming that someone cannot override or bypass segregation of duties, even when pressure or coercion is applied
- carrying out quantitative and qualitative analysis of user permissions to confirm if an individual can complete multiple functions that should be segregated
- confirming that segregation of duties is being applied on all occasions by reviewing a sample of completed requests or claims
- confirming that a review and reconciliation process would identify users who are able to perform multiple functions when they should not be able to
- reviewing any past access breaches to identify how they occurred and how they can be prevented in the future.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Approval workflows
- Data protection
- Defined decision-making powers
- Duplicate prevention
- Privileged system access
- User permissions

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The exploiter
- The organised

Sensitive information access

Limit access to sensitive information and records.

This control targets internal fraud risks.

Examples

Examples of this control include:

- restricting and monitoring access to records of high-profile individuals
- restricting and monitoring access to sensitive information, e.g. commercial in-confidence information
- security classified information being stored in secure environments.

Risks from control gap

Allowing customers, employees or third parties to access sensitive information and records without authority or a business need can lead to:

- the public release of sensitive information
- fraudsters using the information to improperly influence decisions
- fraudsters using the information to coerce others to act, e.g. blackmail
- employees or contractors accessing, manipulating or disclosing sensitive information without authority
- employees or contractors stealing physical documents or records.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that employees understand what sensitive information is
- confirming that processes comply with the Protective Security Requirements
- confirming that there is a process for requesting and approving access to sensitive information
- confirming that employees are aware of the processes to limit access to sensitive information

- confirming procedures for requesting access to sensitive information are robust and actively testing them
- confirming that employees have the right level of security clearance to access sensitive information, if applicable
- confirming through testing or a process walkthrough that access controls or processes cannot be circumvented.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Access controls
- Complaints handling
- Data protection
- Incident reporting
- Procedural instructions or guidance
- Sensitive information control
- User permissions

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The enabler
- The exploiter

Sensitive information control

Control sensitive or official information to ensure it cannot leave your organisation's network without authority or detection.

This control targets internal fraud risks.

Examples

Examples of this control include:

- scanning and quarantining suspect emails sent to an external destination
- limiting access to collaboration websites that enable documents to be uploaded
- controlling access to supporting ICT systems, networks (including remote access), infrastructure and applications
- controlling the use of removable and portable storage media and unapproved connected devices, e.g. USB flash drives
- network management practices and procedures to identify and address network structure or configuration vulnerabilities
- using encryption, particularly when transferring information.

Risks from control gap

Allowing information to leave your organisation's network without authority or detection can lead to employees or contractors:

- publicly releasing official, sensitive or classified information
- providing sensitive or classified information to others for dishonest gain, e.g. helping a company win a government contract
- selling sensitive or classified information to criminals and scammers
- using sensitive or classified information to commit fraud themselves.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- conducting pressure testing to assess if sensitive information release would be prevented or detected by current controls

- consulting subject matter experts about information loss protection controls
- conducting a process walkthrough by sitting with an employee while they show you how the controls work
- reviewing the controls to determine if they would prevent or detect different methods of information disclosure
- validating that information protection controls meet the Protective Security Requirements expectations
- confirming controls are always on and automatically applied
- confirming that detection tolerances or parameters are appropriate
- confirming that detection parameters or thresholds are not widely known
- arranging or reviewing results of technical testing to confirm controls are working to specifications
- confirming that the systems or processes underlying the information loss protection controls are adequate and reliable
- confirming that information or data breaches go to the most appropriate employees or team for review
- reviewing a sample of detected incidents
- analysing reports related to information loss protection controls, e.g. how many breaches are reported and how often
- reviewing who has access to change the controls
- confirming that someone cannot manipulate the information loss protection controls and testing this if required
- checking what other reporting occurs, e.g. whether executives review information or data disclosure reports during committee meetings.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Access controls
- Data protection
- Privileged system access
- Sensitive information access

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The enabler
- The exploiter
- The organised

Specific and consistent processes

Ensure requests or claims use a specific form, process or system for consistency.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- all updates to provider bank accounts are processed using a designated system
- all assets are requested through a specific process or form
- all supplier onboarding requests follow the approved procurement process
- all expense claims are lodged using the designated expense management system
- all grant applications are completed using the official application form
- all payroll adjustments are entered and approved through the payroll system only.

Risks from control gap

Not using a specific form, process or system to manage requests or claims can lead to:

- disorganised practices
- inconsistent decision making
- less transparency and ability to track decisions and past processes
- weaknesses in other fraud controls
- fraudsters deliberately using confusion and deception to exploit dysfunctional or inconsistent processes.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- analysing completed requests and claims to confirm the specific form, process or system was used on all occasions

- reviewing a sample of completed requests and claims to confirm the specific form, process or system was used on all occasions
- undertaking testing or a process walkthrough to confirm that processes cannot be circumvented
- reviewing procedures or guidance to confirm they clearly specify the form, process or system to be used
- confirming forms, processes or systems are always available
- asking employees about the forms, processes or systems to make sure they have a consistent understanding
- confirming that someone cannot get past the requirement to use a specific form, process or system, even when subject to pressure or coercion.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Access controls
- Data protection
- Privileged system access
- Procedural instructions or guidance
- Trained and qualified employees

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The enabler
- The exploiter
- The fabricator
- The impersonator

System testing

Conduct system testing to identify vulnerabilities prior to release.

This control targets internal fraud risks.

Examples

Examples of this control include:

- testing all new systems or system updates as part of the ICT system lifecycle or change management process
- conducting user acceptance testing to test for fraud risks or control vulnerabilities
- performing vulnerability assessments and penetration testing on systems.

Risks from control gap

Fraudsters could take advantage of untested systems to create loopholes for:

- facilitating fraudulent payments
- accessing, manipulating or releasing sensitive information
- erasing records of their activities to avoid detection.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- undertaking a desktop review of testing policies and processes to confirm that clear and consistent processes exist
- confirming that testing processes meet approved policies and accepted standards
- confirming that the results of system testing are documented and reviewing the documentation
- consulting subject matter experts on testing processes and systems to evaluate their understanding and thoughts about fraud control
- confirming that testing processes would identify specific types of vulnerabilities, e.g. malicious code

- conducting a system walkthrough by having employees show you a process
- reviewing who has access to perform testing
- reviewing the system permissions needed to perform testing
- confirming that testing environments accurately replicate production environments
- reviewing how the results of system testing are reported and rectified as required
- confirming that defects or other issues are adequately resolved
- confirming that post-production testing also occurs.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Automatic data matching
- Internal audits or reviews
- Procedural instructions or guidance
- Quality assurance checks
- Sensitive information control
- Sufficient resourcing

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The enabler
- The exploiter

User permissions

Assign permissions to users based on specific business needs.

This control targets internal fraud risks.

Examples

Examples of this control include:

- limiting access to certain functions to specific permissions within systems
- requiring a business case and approval to obtain specific permissions
- making sure only teams who require it have access to certain functions, e.g. only payroll employees having access to payroll functions and information
- blocking employees from accessing their own records
- only allowing authenticated clients or authorised representatives to perform functions on a client's record.

Risks from control gap

Not controlling user permissions can lead to:

- employees facilitating fraudulent payments
- employees accessing, manipulating and disclosing information without a business need
- employees processing fraudulent requests or claims for themselves or another person
- criminals coercing employees into providing information.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming the existence of permissions and limits within the system
- reviewing procedures or guidance to confirm they clearly specify where permissions should be limited
- obtaining and reviewing requirements for who should have certain user permissions

- confirming the existence of a request and approvals process for obtaining specific permissions
- confirming request and approvals processes are consistently applied
- confirming that employees moving roles within the organisation do not automatically take their access or permissions with them
- reviewing procedures for requesting user permissions, confirming the request processes are robust and actively testing them if required
- confirming that someone cannot circumvent standard process requirements, even when subject to pressure or coercion
- confirming that user permissions consider segregation of duties requirements
- reviewing the need for security clearances for some permissions
- reviewing reports of user permissions to confirm only those who require them have the permissions
- undertaking testing or a process walkthrough to confirm that permissions within systems work correctly and cannot be circumvented
- confirming the existence of a review and reconciliation process and reviewing the reports
- reviewing any past access breaches to identify how they occurred
- checking that permissions for employees who have resigned or changed roles are promptly removed.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Access controls
- Data protection
- Eligibility requirements
- Escalation procedures
- Identity verification
- Parameters and limits
- Privileged system access
- Segregation of duties

- Sensitive information access
- Sensitive information control

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The enabler
- The exploiter
- The impersonator

Watchlists

Restrict access by blocking items on a designated list until additional verification is completed.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- blocking suspect bank accounts so they cannot be used for a client, provider or vendor receiving funding
- making grey-listed providers go through additional suitability checks before being registered
- providing an approved list of providers or vendors who have already been vetted.

Risks from control gap

Not using watchlists can lead to fraudsters:

- operating or moving across different government programmes without detection
- reusing methods, e.g. compromised identities to access accounts
- using the same bank account to hijack multiple payments.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- conducting fraud control testing to confirm that the watchlist works as intended
- consulting subject matter experts about the watchlists
- reviewing policies or other documentation related to the watchlists
- conducting a process walkthrough to observe how the watchlists are used
- undertaking analysis of data and reports related to the watchlist, e.g. reviewing reports to see how many blocks are reported and how often

- confirming the watchlists are always on and automatically applied
- confirming that the systems or processes underlying the watchlists are adequate and reliable
- confirming that attempts to use listed information are flagged and reviewed
- confirming that watchlist information is not widely known or accessible
- confirming that someone cannot manipulate the lists, even when pressure or coercion is applied
- confirming that access to the lists is monitored and reviewed
- confirming that the lists are kept up to date.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Automatic data matching
- Coordinated disruption activity
- Identity verification
- Mandatory information
- Strategic partnerships
- System testing

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The exploiter
- The fabricator
- The impersonator
- The organised

Detection controls

Detection controls are designed to identify instances of fraud and corruption once they have occurred, enabling timely intervention to limit their impact. While prevention controls aim to stop misconduct from happening, detection controls provide a critical second line of defence by increasing the likelihood that fraudulent activity will be discovered.

Effective detection controls are typically risk-based, focusing on areas with higher exposure to fraud and using both manual and automated techniques to identify anomalies, patterns or red flags. They enable organisations to respond quickly, disrupt fraudulent activity and prevent further loss or harm, and provide valuable insights into control weaknesses and emerging risks.

When combined with clear escalation pathways and investigation processes, detection controls help ensure that incidents are managed consistently, transparently and effectively.

Activity reporting

Prepare summary reports on activities for clients, managers or responsible employees.

This control targets internal fraud risks.

Examples

Examples of this control include:

- reporting on programme or administrative budgets and expenses
- reporting on programme claims, payments and other key performance indicators
- reporting on employees' attendance and allowances, e.g. overtime payments
- reporting on project or contract performance
- reporting on procurement and vendor payments
- reporting to clients and employees on:
  - changes to their accounts
  - programme or organisational performance
  - programme or organisational change
  - trends and issues.

Risks from control gap

Not reporting on activities can lead to:

- decreased transparency of actions and outcomes
- poor management of performance, decision making and risk
- less action and accountability to prevent, detect and respond to fraud and corruption
- diminished capability to detect fraudulent activity and respond to it
- clients, employees or contractors taking advantage of obscurity to commit fraud, act corruptly and avoid exposure
- clients, employees or contractors being confused about requirements and accidently or recklessly engaging in non-compliant conduct that could lead to fraud.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that reports are produced and used
- reviewing a sample of reports to determine if they are clear, relevant and would help someone to detect fraud
- reviewing data related to reports to see how often they are reviewed
- confirming that reports and data cannot be manipulated
- confirming that reports are sent or readily available to the appropriate people, e.g.:
  - customers who can view reports via their online account
  - line managers who receive the report via email
  - executives who review reports during committee meetings.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Accurate information collection
- Audit logging
- Exception reporting
- Incident reporting
- Specific and consistent processes

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The fabricator
- The impersonator

Automatic change notifications

Automatically notify clients or employees about high-risk changes to alert them to potential fraud and avoid delays in disrupting or investigating an incident.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- system-generated notifications of high-risk events or transactions, e.g. when:
  - contact details are changed
  - bank accounts are changed
  - system accesses are updated
  - payments are made
  - claims or requests are processed.

Risks from control gap

Allowing high-risk events or transactions to occur without automatically notifying clients or employees can lead to:

- fraudulent activity going unnoticed
- fraudsters feeling more confident their actions will not be detected
- delays in investigations and responses
- additional opportunities for fraud.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- testing high-risk activities and transactions to confirm that notifications are being sent
- analysing data related to automatic notifications and comparing it to events or transactions
- evaluating the method and destination of notifications to determine if they are sent to the most appropriate person using the best method

- confirming that notifications cannot be modified, stopped, redirected or prevented from arriving, and testing the controls if required
- considering the timeliness of notifications, e.g. when they are sent or when they would be received, and if this would provide sufficient time to respond to potential fraud
- reviewing the notification to determine if messages are clear and relevant to the receiver.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Automatic data matching
- Complaints handling
- Exception reporting
- Sensitive information access
- Specific and consistent processes

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The exploiter
- The fabricator
- The impersonator
- The organised

Automatic data matching

Match data automatically with another source to obtain or verify details relevant to the request or claim.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- comparing claim or recipient data in a batch file with a corresponding data file
- populating claim data automatically by using a data link
- matching programme participants by sharing data files between organisations.

Risks from control gap

Not matching data with another source can lead to:

- the inability to obtain or verify information
- false information being used to support a request or claim
- changes or information that would affect entitlements not being disclosed
- changes in circumstances being missed
- individuals providing false information to support a request or claim
- individuals failing to disclose changes or information that would affect their entitlement.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- consulting subject matter experts about the data matching process
- reviewing the accuracy of the data match by doing quantitative analysis, e.g. the percentage of successful matches
- undertaking quantitative analysis to determine the reliability of the data match, e.g. the data is reliable or trustworthy

- reviewing the usefulness of the data match by doing qualitative analysis of the data and measuring its impact on data matching
- confirming that data matching is working correctly by comparing a sample of completed requests or claims to the data matching information
- confirming that the original data sources are impartial, reliable and trustworthy
- confirming that data matching is used to support decision making by doing a process walkthrough
- confirming data matching is always on and available
- confirming that employees cannot bypass data matching, even when subject to pressure or coercion.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Accurate information collection
- Automatic prompts and alerts
- Coordinated disruption activity
- Data protection
- Eligibility requirements
- Escalation procedures
- Mandatory information
- Procedural instructions or guidance
- Strategic partnerships
- Trained and qualified employees
- Watchlists

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The enabler
- The fabricator
- The impersonator
- The organised

Avenues for reporting fraud

Put in place processes for employees or external parties to lodge tip-offs or provide protected disclosures.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- a dedicated reporting line
- an online form available through an internal or external website
- avenues for protected disclosures if there is suspected wrongdoing within organisations.

Risks from control gap

Not having discreet or confidential ways for employees or external parties to report fraud and corruption can lead to:

- an unethical workplace culture
- fraudsters feeling confident that their actions will not be detected
- reduced ability to detect and respond to fraud or corrupt activity
- reduced action and accountability for preventing, detecting and responding to fraud and corruption
- systemic fraud or corruption.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that a consistent process exists for reporting fraud and corruption
- confirming that the process for reporting fraud and corruption is easy to find and understand
- confirming that the options for reporting fraud and corruption are clearly communicated
- considering if the processes in place support the person reporting fraud and corruption

- confirming if processes are compliant with the Protected Disclosures Act 2000
- reviewing any cases where reporting did not result in follow-up action to see if changes are required for how and what information is obtained after an allegation of fraud
- confirming that processes allow employees or external parties to report different types of fraud and corruption
- confirming that processes can accommodate reports from a variety of sources, e.g. external individuals, employees, vendors and other organisations.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Complaints handling
- Ethical culture
- Fraud awareness training
- Governance and oversight
- Sufficient resourcing

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The enabler
- The exploiter
- The fabricator
- The impersonator
- The organised

Complaints handling

Allow clients, employees and third parties to lodge complaints about actions or decisions they disagree with.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- allowing clients, employees and external parties to make complaints or raise concerns about:
  - issues with payments, e.g. unexpected delays
  - issues they experience with services
  - the conduct or operations of service providers or other third parties
  - a procurement outcome
  - a recruitment outcome
  - the conduct of others in the workplace
- training employees to look for fraud and corruption, e.g. cartel behaviour, when reviewing complaints
- creating a complaints management strategy that outlines how to resolve a complaint and provide feedback to the person who made the complaint
- storing, collating and sharing complaint information for intelligence and detection purposes.

Risks from control gap

Having no clear process for making complaints can lead to:

- disgruntled employees, clients or third parties becoming motivated to commit fraud or rationalising fraudulent or corrupt behaviour
- fraud or corrupt activity going unnoticed or unchallenged
- delays in investigations and responses
- unknown systemic fraud or corruption.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming the process for making complaints is easy to locate and use
- measuring how long it would take to receive a complaint and respond to potential fraud
- confirming that a consistent process exists for making and handling complaints
- confirming the options for lodging complaints are clearly communicated, e.g. providing a dedicated phone number
- confirming that complaints are adequately investigated
- confirming that clear processes exist for referring cases of potential fraud for investigation
- confirming that clients, employees or third parties would be able to notice changes that are different from what is standard, normal or expected.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Automatic change notifications
- Avenues for reporting fraud
- Incident reporting
- Quality assurance checks
- Sufficient resourcing

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The enabler
- The exploiter
- The fabricator
- The impersonator
- The organised

Evidence and document capture and storage

Capture documents and other evidence to detect, analyse, investigate and disrupt fraudulent activity.

This control is supported by the information and records management standard and the Public Records Act 2005.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- storing all claims forms on a secure system
- scanning and uploading all evidence for a claim into a secure system
- documenting decisions on a secure system before processing the request or claim
- keeping all procurement decisions and documentation on file.

Risks from control gap

Poor or absent capture and storage of documents and evidence can lead to:

- difficulty in detecting, analysing, investigating and disrupting fraudulent activity
- failure of criminal, civil or administrative actions due to inadmissible evidence
- inability to share information with other organisations
- information being improperly accessed or released.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that the capture and storage of documents and evidence follow the information and records management standard

- confirming that investigators understand what the evidence requirements are and that they have access to evidence
- confirming that evidence is sufficiently captured by investigators to support an investigation
- confirming that storage of evidence is automatic and reliable
- confirming that employees understand the processes for storing documents and chain of custody of evidence
- confirming that access to documents is restricted to those who need it for business purposes
- confirming that documents cannot be altered and that the original is retained
- confirming that audit logging is automatically generated when accessing or updating documentation
- confirming that investigators can access evidence held by another party, if required.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Audit logging
- Data protection
- Managerial or independent oversight
- Procedural instructions or guidance
- Specific and consistent processes
- Watchlists

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The enabler
- The fabricator
- The organised

Exception reporting

Produce exception reports to identify activities that are different from the standard, normal or expected process and should be further investigated.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- unusually high payments
- large salary changes
- unusually high programme payments
- excessive ordering of assets
- employees who have made more expense claims than usual in a month
- prices that do not match market variations
- payments or claims repeatedly just below reporting thresholds
- claims that exceed a set frequency or threshold.

Risks from control gap

A lack of exception reporting can lead to:

- disorganised or inconsistent practices and decision making
- less transparency of actions and outcomes
- poor management of fraud and corruption risks
- less action and accountability to prevent, detect and respond to fraud and corruption
- fraud or corrupt activity going unnoticed or unchallenged.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that the exception tolerances or parameters are appropriate

- confirming that the exception parameters or thresholds are not widely known
- confirming that exception reports are produced and used, and that the process is adequate
- confirming that exception reports go to the most appropriate team or employee for review
- walking through processes with employees while they review reports and respond to anomalies
- reviewing a sample of reports to see if they are clear, relevant to the user and would help to detect fraud
- reviewing statistics related to reports, e.g. the quantity and frequency of exceptions that are reported
- reviewing who has access to exception reports
- confirming that someone cannot manipulate exception reports or the data they are based on.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Accurate information collection
- Activity reporting
- Automatic data matching
- Incident reporting
- Parameters and limits

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The enabler
- The exploiter
- The fabricator

Fraud detection software

Use fraud detection software to automatically analyse data to detect any anomalies that may indicate fraud or corruption.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- analysing system access logs to detect unauthorised access to internal systems or online accounts
- monitoring for suspicious changes to client or provider bank accounts, e.g. accounts being used more than once or for multiple clients
- monitoring the use of compromised personal identity information
- analysing bulk data sets to identify suspicious patterns and anomalies
- automating reviews of system access logs to detect unauthorised access
- analysing claims data to identify suspicious patterns and anomalies.

Risks from control gap

Not using fraud detection software can lead to:

- reduced transparency
- a belief among fraudsters that they will not be caught
- not identifying fraudulent or corrupt activity
- difficulty in early detection, investigation and response to allegations of fraud.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- conducting pressure testing to determine if fraudulent activity would be detected
- confirming if subject matter experts are confident about how the detection programme operates

- confirming that the detection programme settings are not widely known, allowing someone to deliberately avoid detection
- confirming that the data or logs underlying the detection programme are adequate and reliable
- confirming that detection programme reports are produced and used, and the process is adequate
- confirming that detection programme results go to an independent and appropriate reviewer
- reviewing a sample of detected incidents to identify areas to improve processes.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Accurate information collection
- Audit logging
- Automatic data matching
- Data protection
- Evidence and document capture and storage
- Exception reporting
- Record reconciliation
- Recovery and debt management processes
- Watchlists

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The exploiter
- The fabricator
- The impersonator
- The organised

Incident reporting

Report on incidents or breaches to help identify if further investigation is required.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- reporting of financial breaches, e.g. failure of an employee to reconcile a credit card on time
- reporting of system security incidents and breaches
- employees reporting lost, stolen or damaged assets
- employees reporting security incidents, e.g. loss of classified documents.

Risks from control gap

A lack of reporting on incidents and breaches can lead to:

- disorganised or inconsistent practices and decision making
- less transparency over actions and outcomes
- poor management of performance, decision making and risk
- less action and accountability to prevent, detect and respond to fraud and corruption
- poor workplace culture that fails to identify or report fraud or corrupt activity
- fraud or corruption going unnoticed or unchallenged.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that the reporting requirements for incidents are appropriate
- confirming that reports are actually produced and used
- reviewing a sample of reports to determine if they are clear, relevant and would help someone detect fraud

- confirming that documents outlining the process for reporting incidents are easy to locate and use
- confirming the options for reporting incidents are clearly communicated
- reviewing statistics related to reports to identify how many incidents are reported and how often
- confirming that incident reports go to the most appropriate employees or team
- reviewing who has access to incident reports
- checking what other reporting occurs, e.g. if executives review reports during committee meetings.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Automatic change notifications
- Avenues for reporting fraud
- Complaints handling
- Escalation procedures
- Fraud investigation policy

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The enabler
- The exploiter
- The fabricator
- The impersonator
- The organised

Information verification

Verify key information from requests or claims with an independent and credible source.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- cross-referencing the provider number with provider register(s)
- verifying claim eligibility by cross-referencing details held by another programme or organisation
- requesting original or certified documents instead of photocopies or screenshots
- obtaining corresponding evidence from both a client and provider
- verifying academic and professional qualifications with the education provider
- confirming business details.

Risks from control gap

Not verifying the information that you receive can lead to:

- fraudsters providing false information or evidence to support a request or claim
- fraudsters hiding information that would affect their entitlements
- fraudsters successfully using forged documents to support a request or claim
- difficulties in responding to fraud.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that reference and guidance materials regarding information verification processes are easy to understand
- confirming that information is verified by reviewing a sample of completed requests or claims

- confirming that processes cannot be circumvented by doing pressure testing or a process walkthrough
- reviewing procedures and guidance to confirm they clearly specify the requirements for verifying information
- confirming that employees have a consistent and correct understanding of how to verify information
- confirming that verification requirements are clearly communicated to employees, customers and third parties
- confirming that employees cannot bypass or manipulate the verification requirements, even when pressure or coercion is applied
- confirming that employees receive training about how to verify information.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Automatic data matching
- Coordinated disruption activity
- Eligibility requirements
- Mandatory information
- Strategic partnerships
- Sufficient resourcing
- Trained and qualified employees
- Watchlists

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The fabricator
- The impersonator
- The organised

Internal audits or reviews

Conduct internal audits or reviews to evaluate and improve the effectiveness of risk management, control and governance processes.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- regular security audits of ICT
- programme performance audits
- random site visits for providers
- surveys to check the accuracy of regular payments
- monthly audits of employee travel expenditure
- regular reviews of grants allocations
- regular audits of credit card spending.

Risks from control gap

A lack of regular audits or reviews of activities can lead to:

- clients, employees, or contractors taking advantage of weaknesses in programmes and systems to commit fraud, act corruptly and avoid exposure
- reduced levels of compliance and increased errors due to inconsistent and unclear processes, rules and decision making
- fraudsters more easily committing fraud, due to inconsistent practices and processes being in place, and no fear of being exposed or prosecuted
- less transparency over the actions and decisions of employees and third parties
- increased opportunities for employees or contractors to take advantage of positions of trust to act corruptly, commit fraud and avoid exposure
- decreased ability to detect and respond to fraud or corrupt activity

- decreased accountability to prevent, detect and respond to fraud and corruption
- reduced ability to detect systemic fraud or corruption.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- reviewing the outcomes of audits or reviews
- confirming that audits or reviews are carried out
- checking that audits or reviews are performed regularly
- confirming that the scope of audits or reviews consider fraud risks and controls
- confirming that audits or reviews are independent, completed by qualified persons and are resilient to corrupting influences
- checking what other reporting occurs, e.g. executive reviews of reports during committee meetings.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Audit logging
- Evidence and document capture and storage
- Governance and oversight
- Managerial or independent oversight
- Record reconciliation

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The exploiter
- The fabricator

Quality assurance checks

Conduct quality assurance checks to confirm that processes are being followed correctly and to a high standard, and/or that goods received are what they are claimed to be.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- randomly selecting work to quality check, e.g. 2% of processed claims or decisions
- having an independent person quality check high-risk activities on all occasions, e.g. changes to vendor records
- having the procurement team quality check purchase orders above $10,000 before they go to the spending approver
- selecting random or targeted samples of products to check that they are what they are claimed to be.

Risks from control gap

A lack of quality assurance checks can lead to:

- reduced levels of compliance and increased errors due to inconsistent applications of processes, rules and decision-making
- decreased transparency of actions and decisions made by employees and third parties
- mismanagement of performance, decision making and risk
- decreased detection and response to fraud or corrupt activity
- goods and services that are unsafe or not fit for purpose being received by organisations or the public
- clients, suppliers or businesses providing faulty goods or services anywhere in the supply chain process.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- reviewing quality assurance processes to see if they align with quality assurance policies and standards
- comparing data related to quality checks and measuring results against key performance indicators
- reviewing quality checking processes to determine if the checks would identify fraud
- confirming that employees know what quality assurance checks they need to do by doing a process walkthrough
- confirming that employees understand how to perform quality assurance checks correctly and consistently by carrying out interviews, workshops and surveys
- confirming that processes for high-risk activities include an independent review aspect, e.g. reviews by employees in other locations
- confirming that processes are standardised across team members by comparing completed work from various employees.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Defined decision-making powers
- Fraud awareness training
- Governance and oversight
- Managerial or independent oversight
- Procedural instructions or guidance
- Specific and consistent processes
- Sufficient resourcing

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The enabler
- The exploiter
- The fabricator

Record reconciliation

Reconcile records and accounts to detect if something is different from what is standard, normal or expected, which may indicate fraud.

This control targets both internal and external fraud risks.

Examples

Examples of this control include reconciling records by comparing:

- travel approvals produced each month with the trips booked using a travel vendor
- credit card expenses against required receipts
- overtime budgets matched against spending
- proof of assets ordered versus assets received.

Risks from control gap

A lack of records and account reconciliation can lead to:

- fraudsters feeling more confident their actions will not be detected
- high levels of non-compliance or errors due to inconsistent and unclear processes, rules and decision making
- less transparency over the actions and decisions of employees and third parties
- fraud or corrupt activity going unnoticed or unchallenged.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that the reconciliation is segregated from the processing, e.g. ensuring that one employee cannot process and reconcile the same activity
- reviewing who has access to complete the reconciliations
- walking through the process with an employee while they complete a reconciliation

- confirming a consistent reconciliation process exists
- confirming that records cannot be manipulated
- reviewing the reconciliation process to ensure it would identify different methods of fraud
- conducting interviews, workshops or surveys with employees who complete reconciliations to assess their understanding and feedback about fraud control policies
- checking if and how reconciliation results are reported.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Automatic data matching
- Duplicate prevention
- Evidence and document capture and storage
- Information verification
- Internal audits or reviews

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The fabricator
- The impersonator

Response controls

Response controls are activated once fraud or corruption has been detected, and are critical in minimising harm to the organisation, its people and its reputation. These controls focus on taking timely, structured and proportionate action to contain the issue, address its root causes and ensure that appropriate consequences are applied.

Key response activities include conducting thorough and impartial investigations to establish the facts. Depending on the outcome, organisations may pursue disciplinary action, termination of employment or referral to external authorities for prosecution. Recovery actions are also important to mitigate financial loss and demonstrate accountability.

Audit logging

Maintain audit logs of staff, client or third-party interactions to help with fraud investigations and deterrence.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- setting up audit logging by capturing information like:
  - access to systems for audit purposes
  - changes to data and who made the changes
  - access to sensitive information
  - access and use of high-risk accounts and transactions.

Risks from control gap

Poor or no audit logging can lead to:

- difficulty in detecting, analysing, investigating and disrupting fraudulent activity
- insufficient data not being able to support an investigation.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that audit logging is switched on
- reviewing the logs to confirm they capture sufficient and meaningful information to support detection or an investigation
- conducting random and targeted reviews of audit logs
- checking that the method of logging is reliable
- confirming and testing (if required) that audit logs are stored securely
- confirming that audit logs are available to investigators
- confirming that audit logs cannot be switched off, deleted or altered, even by staff with privileged access

- if audit logs can be altered, confirming that these actions are also logged and that copies of originals are retained
- confirming that audit logs are retained as per the relevant records authority.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Data protection
- Evidence and document capture and storage
- Privileged system access
- Specific and consistent processes
- System testing

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The deceiver
- The exploiter
- The fabricator
- The impersonator

Coordinated disruption activity

Coordinate disruption activities across multiple programmes or agencies to strengthen processes for identifying serious and organised criminals.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- revoking funding approvals
- deregistering businesses and individuals
- conducting tax assessments
- sharing information with other agencies to support due diligence processes
- referring cases to the relevant law enforcement agency when evidence of criminal activity is detected or suspected.

Risks from control gap

Poor or no coordinated disruption activities can lead to:

- criminals repeatedly exploiting programmes
- criminals shifting focus and exploiting new programmes
- criminals exploiting multiple programmes
- organised criminal groups using sophisticated methods to systematically target government programmes
- agencies overlooking complex, organised offending by focusing only on opportunistic fraud.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- understanding the organisation's capability to disrupt complex criminal fraud by consulting with analysts, investigators and other experts about the process

- checking that disruption activities targeting a specific type of fraud have been implemented and completed in previous cases
- retrieving and analysing data related to a specific fraud, e.g. the number and type of actions taken.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Fraud investigation policy
- Governance and oversight
- Penalties for fraud and non-compliance
- Recovery and debt management processes
- Strategic partnerships

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The enabler
- The organised

Fraud investigation policy

Investigate fraud in line with your organisation's investigation policy.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- documenting the responsibilities and procedures to be followed when fraud is suspected
- creating governance and oversight of cases referred for criminal investigation, prosecution or disciplinary action.

Risks from control gap

Conducting investigations without having a fraud investigation policy can lead to:

- reduced effectiveness of investigations
- poor response times
- contamination and/or loss of evidence
- reduced likelihood of prosecutions
- individuals being encouraged to commit fraud if they think the chance of a successful prosecution is low
- suspects and/or innocent third parties being unfairly treated.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming that the investigation policy conforms with best practice, is subject to periodic review and was followed for completed investigations
- confirming that investigations were completed by qualified persons
- confirming that processes were in place to identify and manage potential bias and conflicts of interest, and ensuring investigators were resilient to corrupting influences

- confirming that investigation actions, findings and subsequent decisions were within the defined scope and accurately recorded
- confirming that chain of custody and evidence handling requirements were followed for the storage, access and management of evidence
- confirming that investigation outcomes were appropriately escalated, including referral to law enforcement
- confirming that investigators and those who review investigation reports receive regular training on the policy
- testing and confirming personal and sensitive information gathered during an investigation is appropriately stored to protect confidentiality and privacy
- analysing investigations data to determine patterns, e.g. the number of cases referred for investigations compared to the allegations received.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Defined decision-making powers
- Evidence and document capture and storage
- Governance and oversight
- Trained and qualified employees

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The enabler
- The exploiter
- The fabricator
- The impersonator
- The organised

Penalties for fraud and non-compliance

Penalise customers, staff or third parties that commit fraud or do not comply with rules, processes and expectations.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- raising debts, penalties and interest payments for clients who commit fraud or do not comply with requirements
- fining, suspending or cancelling providers or third parties who commit fraud or do not comply with requirements or standards
- sanctioning or terminating staff for misconduct or fraud
- penalties for contractor misconduct or unreasonable failures to meet contract obligations.

Risks from control gap

A lack of penalties for fraud and non-compliance can lead to:

- individuals not being deterred from committing fraud
- fraud increasing over time
- repeated or systemic non-compliance or criminals reoffending .

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- reviewing the results of compliance reviews or fraud investigations to confirm that penalties are:
  - enforced, e.g. debts raised, termination, prosecution
  - appropriate for the type of fraud
  - consistent across similar cases
  - recorded against the customer, vendor, staff member or contractor records

  - reported on
  - shared with other parties who need to know, e.g. other departments are notified of serious or organised fraud, or staff or contractor terminations for fraud or misconduct
- analysing statistics and reports on repeated non-compliance or criminals reoffending
- confirming that controls are in place to disrupt repeated non-compliance or criminals reoffending.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Recovery and debt management processes
- Separation and termination processes
- Strategic partnerships

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The enabler
- The exploiter
- The fabricator
- The impersonator
- The organised

Recovery and debt management processes

Implement processes that identify and recover debts owed by employees, customers and third parties due to non-compliance.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- retrieving incorrect or fraudulent payments with the help of financial institutions
- recording and recovering debts arising from non-compliance
- recording and recovering employee overpayments
- obtaining refunds from suppliers if contract obligations are not met
- working with the New Zealand Police Financial Crime Group
- making a referral to the New Zealand Police Asset Recovery Unit if it is believed that there may be proceeds of crime involved
- requiring vendors to provide a rebate if contract obligations are not delivered or fraud occurs
- including clawback clauses in contracts and agreements.

Risks from control gap

A lack of recovery and debt management processes can lead to:

- being unable to identify or recover debts
- individuals not being deterred from committing fraud
- increasing levels of fraud over time
- repeated or systemic non-compliance or criminals reoffending
- improper debts being raised
- fraudsters avoiding financial consequences .

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- confirming the necessary legislation, policy, processes and/or systems exist to support the recovery of stolen funds or fraudulent payments
- reviewing debt recovery processes to see if they conform to national guidelines and frameworks
- reviewing data on debt recovery
- confirming that statistics on debt recovery are captured by reporting
- determining the timeframes for recovering stolen funds or fraudulent payments. Consider if delays would reduce the recovery of funds.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Counter fraud messaging
- Declarations
- Eligibility requirements
- Fraud awareness training
- Penalties for fraud and non-compliance
- Procedural instructions or guidance

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The enabler
- The exploiter

Separation and termination processes

Put in place processes to properly close an individual or organisation's engagement or involvement with an agency or programme.

This control targets both internal and external fraud risks.

Examples

Examples of this control include:

- using checklists to ensure all access, equipment and responsibilities are closed out for former employees and contractors
- terminating staff or contractors for fraud or misconduct
- cancelling registrations if providers are found to be involved in fraud or misconduct
- removing suppliers from a procurement panel due to fraud or misconduct.

Risks from control gap

Unclear or inconsistent separation and termination processes can lead to:

- insider threats
- dysfunctional workplace cultures
- previous employees retaining access to systems
- fraudsters being reemployed
- suppliers not being properly deregistered and re-entering the system.

Assessing effectiveness

Methods to evaluate the effectiveness of this control include:

- reviewing processes and/or guidelines for termination or separation
- confirming that employees, contractors or providers would be terminated or expelled for fraud or non-compliance
- confirming that data is captured and reported for all terminations involving fraud or misconduct

- identifying cases where staff members, contractors or providers have been terminated for fraud or non-compliance
- confirming processes are adhered to and reported on when contracts end by making sure:
  - assets are returned
  - system access is revoked
  - building access is revoked (passes are returned)
  - information, documentation and intellectual property is protected
- confirming that reasons for termination are recorded by keeping a permanent record for the customer, staff member, contractor, provider or supplier
- confirming that any request for a serious misconduct disciplinary record made to a previous employer was in line with the Workforce Assurance Model Standards and Privacy Act 2020.

Complementary controls

Other capability, prevention, detection and response controls that can enhance this control's effectiveness:

- Coordinated disruption activity
- Decommissioning and disposal
- Governance and oversight
- Procedural instructions or guidance
- Quality assurance checks
- Specific and consistent processes
- Watchlists

Related fraudster personas

Types of behaviour this control is designed to mitigate:

- The corrupt
- The deceiver
- The enabler
- The exploiter
- The fabricator
- The impersonator
- The organised

Build capability and culture

A robust fraud and corruption control environment is comprehensive, transparent and actively maintained. There is no single solution to managing fraud and corruption risks, and processes need to continually adapt to effectively mitigate rapidly evolving threats.

Although there will always be fraud and corruption, organisations can considerably reduce and manage the risk of it occurring by implementing a range of capability, prevention, detection and response controls.

The Counter Fraud Centre offers a range of resources, webinars, workshops and services free to public sector organisations to help build their counter fraud capability and create an effective counter fraud culture.

Find out more at sfo.govt.nz/counter-fraud/counter-fraud-centre.

Acknowledgement

Where relevant, content has been adapted for the New Zealand context from:

Commonwealth Fraud Prevention Centre, 2023. Fraud Control Catalogue. Australia: Commonwealth Fraud Prevention Centre. https://www.counterfraud.gov.au/library/fraud-control-catalogue [accessed 18 February 2026].

Commonwealth
Fraud Prevention
Centre

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