COUNTER FRAUD CENTRE
Tauārai Hara Tāware

Data Countermeasures

Table of contents

1 Introduction 3

1.1 Overview 3

2 Data Countermeasures 4

2.1 Collect useful data 5

2.2 Data sharing arrangements 6

2.3 Data matching 8

2.4 Data analytics 9

2.5 Confirm supplier identity 10

2.6 Identity matching services 12

2.7 Identity verification services 13

1 Introduction

This is the second of two guides that provide examples of countermeasures that can be used to support the policy and delivery teams to reduce significant fraud and corruption risks.

The first guide is focused on the third principle of fraud control in disaster management, namely: *The business and fraud control should work together to implement low-friction countermeasures to prevent fraud risk where possible,* by providing examples of low-friction countermeasures that your organisation can implement or improve.

This guide is focused on the fourth principle of fraud control in disaster management, namely: *Carry out targeted post-event assurance to look for fraud, ensuring access to fraud investigation resource*, by providing examples of how to use data to support post-event assurance activities.

For more information about effective control of fraud in disaster scenarios visit https://sfo.govt.nz/counterfraud/cfc/resources/guides-and-factsheets/fraud-prevention-in-times-of-crisis

1.1 Overview

This guide contains high level information on seven countermeasures about using data in post-event assurance activities.

Not all countermeasures are appropriate for all organisations. Using this guide, practitioners will be able to determine whether it is appropriate to adopt the countermeasure based on their organisations risk exposure and tolerance.

All seven countermeasures include a description of the countermeasures followed by six sections.

- *'Why this is important in a crisis'* provides context to the reasons the countermeasure helps to reduce the risk of fraud during times of disaster response and recovery.
- *'More about this countermeasure'* provides additional information about the countermeasure.
- *'Consideration for implementation'* provides examples of risk associated with the implementation of the countermeasure.

2 Data Countermeasures

This guide contains **seven know your data countermeasures** and should not be considered an exhaustive list of all detection countermeasures. As with any enterprise, knowing and protecting data is of particular importance in disaster recovery situations.

This knowledge ensures that monies reach the most vulnerable or in need and can assist in highlighting previously unknown areas of risk. Proper controls at this stage can also assist with post event assurance to either retrieve monies paid in error or educate a lesson learned process.

Use this guide to:

- consider whether an organisation is exposed to fraud risks which these countermeasures mitigate against
- identify whether these countermeasures have been or should be in place to mitigate these fraud risks

2.1 Collect Useful Data

Collect a range of consistent and relevant data for analysis

Why this is important in a crisis	Collecting a comprehensive set of data during the application phases or when an individual or organisation amends data relating to its circumstances, can assist when an organisation needs to: ▶ verify identity and assess eligibility for a payment ▶ improve the effectiveness of post-payment assurance activities. The more an organisation knows about an individual or organisations, the greater the visibility of eligibility. Also, any post-payment and debt-raising activities may be more effective.
More about this countermeasure	The higher the number of data points held by an organisation, the greater the effectiveness of data matching exercises between organisations and programmes to better enable the detection of fraud. The assessment of eligibility and subsequent ability to detect fraudulent applications relies on organisations understanding the data they hold and its reliability. Embedding practices to ensure data integrity at the point of engagement will help to mitigate the risk of incomplete data, and data quality issues at post-payment.
Considerations for implementation	Some points of data may be difficult for applicants to provide or organisations to collect immediately following a disaster. Organisations should consider alternative mechanisms for verifying identity or circumstances

2.2 Data Sharing Arrangements

Share information and data to prevent, detect, and respond to fraud

Why this is important in a crisis	Arrangements to share information and data are relevant for any disaster relief and recovery measures that need to identify a person and their circumstances to determine the person's eligibility or level of entitlement. When implemented effectively, internal and external data sharing can be a powerful tool to prevent and detect fraud. Data sharing can also quickly and seamlessly verify information and determine whether a person is eligible to receive disaster relief and recovery support.
More about this countermeasure	Arrangements to share data and information can help organisations: ▶ verify identity and eligibility of claimants – this can also protect New Zealanders from having their identity stolen and misused to commit fraud ▶ prevent claimants illegally accessing multiple supports and services ▶ disrupt fraud networks –if a person has defrauded a government programme in one organisation, they will likely try to defraud a programme in another organisation. Getting consent from individuals and businesses to share their data with other organisations can make the process easier. Information Privacy Principle 11(1(c) of the Privacy Act 2020 provides for the sharing of personal information when a person authorises the sharing in this manner. Organisations can also enter into an Approved Information Sharing Agreement (AISA). An AISA is a formal agreement that allows personal information to be shared between (or within) organisations to deliver public services. See the Privacy Commissioner's website for more information.

Considerations for implementation	Effective arrangements to share data rely on data availability, data quality, and authority to share the data. Some privacy provisions may not allow information sharing or reciprocal sharing. Consult your Legal Services team to explore the legal frameworks. If restrictions exist, look for opportunities available to share information where possible.

2.3 Data Matching

Compare new information with existing data sets

Why this is important in a crisis	By verifying and cross-checking information against multiple data sources, existing internal and external data can be used upfront in a low-friction way to prevent or detect the lodging of inaccurate or fraudulent applications.
More about this countermeasure	Data matching can be used for instance to check whether a business exists or whether an individual is employed (when they claim not to be). Examples include: ▶ check an individual's employment status — verify employment data by matching employee data to employer data held by Inland Revenue (where possible) ▶ check whether a business exists — use the New Zealand Companies Register and Charities Register, and the Charitable Trust Register to verify the nature and legitimacy of a business. Information Privacy Principles 10 and 11 of the Privacy Act 2020 provide for the use and disclosure of personal information for purposes, other than what it was collected for, in limited circumstances. Those circumstances include preventing, detecting, and investigating offences (including fraud and corruption).
Considerations for implementation	Data matching relies on data quality and approved information-sharing agreements being in place between organisations.

2.4 Data Analytics

Use data to identify potential fraud or high-risk areas

Why this is important in a crisis

Some traditional countermeasures become ineffective after a disaster (such as claimants being able to access identity documents). Embedding mature data analytics techniques can help to identify high-risk applications that may have typically failed to progress at an earlier stage because standard countermeasures were no longer in operation.

Data analytics can be used to identify fraud against areas of residual risk not covered by upfront countermeasures. It can also complement upfront prevention countermeasures.

More about this countermeasure

Examples of data analytics include:

- using data to build a holistic view of applicant behaviour across different disaster relief and recovery payment types
- using data to validate information captured at application stage to allow for faster and more accurate decisions about eligibility.

Using data to build a holistic view of applicant behaviour involves analysing how an applicant has historically engaged with an organisation. This can provide insight not only into their eligibility but also into the risk of identity compromise.

Considerations for implementation

The effectiveness of any data analytics work relies on data availability and quality. Organisations can mitigate this risk by enhancing their data integrity and developing data-sharing with relevant partners.

2.5 Confirm Supplier Identity

Use the New Zealand Companies Register and Charities Register, and the Charitable Trust Register to access non-public or public data to identify and verify business details.

Why this is important in a crisis

Fraudsters not only impersonate individuals but also businesses during disasters. Organisations should conduct upfront due diligence checks or post-payment assurance activities of vendors/suppliers onboarded during a disaster.

More about this countermeasure

The New Zealand Companies Register and Charities Register, and the Charitable Trust Register are online tools that organisations can use to search, query, visualise and download New Zealand Business Register data. These registers are relevant to organisations that need to make informed decisions about the suitability of the applicant/recipient.

Organisations can use the data for various purposes, including:

- Service delivery – promoting new government services or grants, informing legislative changes, licensing of business activities and identifying and supporting new business
- Disaster response and recovery – identifying businesses, in a disaster area, that have been affected and those that can provide support
- Procurement – validating a supplier's New Zealand Business Number, identifying local suppliers and tradespeople for council initiatives and conflicts of interest checks
- Compliance activities – validating business details, risk profiling, work planning and site visits.

Considerations for implementation

The tools provide business information only. Organisations should factor in other information when undertaking their due diligence assessments.

While the New Zealand Companies Register and Charities Register, and the Charitable Trust Register searches make it harder, fraudsters can still establish beneficial owners and shell companies to commit fraud.

2.6 Identity Matching Services

Use identity matching services to verify the identity of individuals using existing documents

Why this is important in a crisis	Information matching enables organisation, that need to verify information being provided in an application, to match that information against an existing identity. This provides assurance that a legitimate person is being paid.
More about this countermeasure	Online document and face verification services can help organisations verify the identity of an applicant or recipient using a range of data sources and identity technologies. Information Matching is a Department of Internal Affairs service that compares personal information held in one set of records with personal information held in another set of records for the purpose of producing or verifying information about an individual.
Considerations for implementation	Information matching can only confirm and authenticate the identity of individuals. Information matching does not verify the authenticity of other documents, such as claim evidence, or details about a business. Information matching is only possible when authorised by statutes and when it complies with privacy legislation.

2.7 Identity Verification Services

Use identity verification services to verify the identity of individuals identity online.

Why this is important in a crisis	Identity verification services are an easy and secure way for a person to confirm who they are so they can access government online services for both their personal and business matters. Identity verification services are designed to ensure that organisations can trust the information that is shared. These services make it easier for people to access and use online services offered by both government and the private sector.
More about this countermeasure	RealMe is one example of an identity verification service. The Department of Internal Affairs manages RealMe. The service builds trust and confidence by adhering to New Zealand Government security, identity and privacy legislation.
Considerations for implementation	Identity verification services require a person to have access to the internet, their own email and a document with their photo on it. A person may not be able to register in the available timeframe in a disaster and during its recovery. Organisations cannot stop people from losing or sharing their login or other identity information.

COUNTER FRAUD CENTRE

Tauārai Hara Tāware