



**Counter
Fraud Centre**
TAUĀRAI HARA TĀWARE

Guide to Managing Fraud During Emergency Relief and Recovery

DECEMBER 2024



Counter Fraud Centre

Who We Are

The Counter Fraud Centre - Tauārai Hara Tāware (CFC) is the prevention arm of the Serious Fraud Office (SFO) and leads counter fraud efforts in New Zealand's public sector. We focus on building the public sector's resilience to fraud and corruption.

Our Mission

Our mission is to lift counter fraud culture and capability in the New Zealand public sector. We do this by producing guides and tools for the public sector and working directly with agencies to advise them on implementing effective counter fraud systems.

How We Can Help

Our depth of experience means we are ideally placed to lead counter fraud activities. We share our knowledge and expertise on the causes and impacts of fraud and corruption, and how to effectively mitigate them to reduce harm across the public sector. Our international connections also help us leverage key insights and best practice generated by overseas organisations and agencies.

Wherever you are with your counter fraud efforts, we're here to help. From basic fraud prevention factsheets to specific good practice guides we offer a range of resources and tools to help build capability across your organisation. We also provide customised counter fraud advice, workshops, and opportunities for cross-government engagement.

See our Counter Fraud Centre webpage for more information sfo.govt.nz/counterfraud/cfc or get in touch with us at counterfraud@sfo.govt.nz

Table of Contents

1	About this Guide	2
1.1	Introduction	2
1.2	Purpose of this Guide	2
1.3	Who Should Use this Guide	3
2	Fraud Management in Emergency Situations	4
3	Principles of Fraud Control in Emergency Management	5
4	Principle 1: Accept That There Is an Inherently High Risk of Fraud, and That It Is Very Likely to Happen	6
5	Principle 2: Integrate Fraud Control Resources Into Policy Design and Processes	7
5.1	Integrate Fraud Control Resources	7
5.2	Equip Employees to Prevent and Detect Fraud	8
6	Principle 3: Implement Low Friction Countermeasures	9
6.1	Coordinated Response to Fraud	9
6.2	Application Processes	10
6.3	Reviewing, Approving and Processing Applications	12
7	Principle 4: Carry Out Post-Event Assurance	15
7.1	Types of post-event assurance	15
8	Principle 5: Be Mindful of the Shift Into Longer-Term Services	17
9	Examples of Fraud in Emergency Management	18



1 About this Guide

1.1 Introduction

Emergency relief and recovery is an important function of the New Zealand Government, given the frequency and impact of natural disasters such as floods, droughts, earthquakes and other extreme weather events. Emergency management in New Zealand is generally led by local authorities, co-ordinated regionally by Civil Defence Emergency Management groups and supported nationally by the National Emergency Management Agency (NEMA) and other government agencies.¹

In times of emergency, it is important that the Government provides immediate support to those in affected communities. This might include additional funding to individuals and community groups, emergency accommodation, and the provision of basic supplies.

Immediate support will often involve a trade-off between urgent programme delivery and the implementation of robust fraud controls. As the priority will always be to ensure services and support reaches the people who need them as soon as possible, it can make relief programmes an attractive target for fraudsters.

There are many examples of fraudsters exploiting emergency situations to gain access to services or funding which they are not entitled to ([see page 18 for examples](#)). Understanding how fraud happens and how to effectively manage it can prevent essential funding from being lost to fraudsters and aid in the recovery of money when fraud does occur.

1.2 Purpose of this Guide

Effective emergency management involves anticipating potential risks before emergencies occur and implementing mitigation strategies to manage and minimise their impact. By addressing fraud risk in less time-sensitive environments, more effective countermeasures can be developed and implemented.

This guide includes the principles for fraud control in emergency management and offers practical guidance on managing fraud risks during an emergency response.

¹ Department of Prime Minister and Cabinet, [“Briefing to the Incoming Minister for Emergency Management and Recovery” \(2023\) page 7.](#)

Sections four to eight sets out each of the five principles of fraud control and explains why each principle is important to consider in an emergency management situation. Also included are potential countermeasures that can be implemented before, during and after an emergency to help mitigate the fraud occurring.

Although this guidance emphasises the time-critical aspects of emergency management, it is crucial to consider the risks and threats of fraud throughout the lifecycle of emergency management response.

1.3 Who Should Use this Guide

This guide should be used by people in organisations who are responsible for decision making and distribution of emergency relief funding.

This typically means disaster response agencies, policy professionals, risk practitioners, finance teams and assurance leads. It may also include individuals responsible for evaluating or approving emergency funding requests.



2 Fraud Management in Emergency Situations

Before an emergency occurs planning can help to increase the readiness of an organisation to begin the relief and recovery process. For this reason, emergency management should be thought of as a cyclical process, with as many controls put in place as possible before the emergency arises. This will enable and empower organisations to better manage the associated fraud risks, from the outset of an emergency.

The types of fraud that can arise will depend on the type of emergency. It is important for those developing relief and response policies and processes to recognise where they might be vulnerable. Although the risk of fraud typically increases during an emergency, organisations can still effectively mitigate this risk. Principles 2 to 4 offer guidance on how to achieve this.

Determining the risk appetite for fraud in an emergency response programme is a key responsibility of the person assigned to manage fraud risk. As highlighted by the Office of the Auditor General, *“In the interests of getting funding quickly to affected people, this heightened risk will need to be tolerated to some degree... It is important to establish the “risk appetite” (that is, the level of risk a public organisation is willing to accept) early. Without clarity on the risk appetite, it is difficult to make informed decisions about the scale and scope of the pre- and post-payment protections to put in place.”*²

² Office of the Auditor General Report, “Management of the Wage Subsidy Scheme” (2021), page 32.


3 Principles of Fraud Control in Emergency Management

When fraud goes unmanaged, it can have significant negative impacts. This includes reducing resources available to affected communities, increasing costs of relief efforts and undermining community confidence in the organisation(s) involved in the response.

The principles outlined below have been developed by the International Public Sector Fraud Forum (IPSFF)³ and offer practical ways to plan for and manage fraud risk in emergency situations.

1	Accept there is an inherently high risk of fraud, and that it is very likely to happen.	Organisations need to be prepared, look for, and address fraud concerns before, during and after an emergency event.
2	Integrate fraud control resources (personnel) into the policy and process design to build awareness of fraud risks.	Involve skilled and experienced fraud personnel to identify, record, manage and report fraud risk.
3	The business and fraud control teams should work together to implement low friction countermeasures to prevent fraud risk where possible.	Once they understand some of the risks of fraud and corruption, the fraud control personnel should actively support the policy and delivery teams by suggesting key countermeasures that could reduce fraud risks, while ensuring minimal delay to payments or services.
4	Carry out targeted post-event assurance to look for fraud, ensuring access to fraud investigation resources.	Where the implementation of up front, preventative, countermeasures can be limited; post-event activities should be carried out to mitigate potential fraud risks.
5	Be mindful of the shift from emergency payments into longer term services and revisit the control framework, especially where large sums are invested.	When the initial time-pressured response ends, more systematic fraud risk processes should begin for any longer term services and support (for example, moving into the rebuilding phase).


³ The IPSFF consists of representatives from organisations in the governments of Australia, Canada, New Zealand, the United Kingdom and the United States. The collective aim of the forum is to come together to share best and leading practice in fraud management and control across public borders.



4 Principle 1: Accept That There Is an Inherently High Risk of Fraud, and That It Is Very Likely to Happen

During emergency relief and recovery situations, there is a higher risk of fraud and corruption due to several factors:

- **High trust approach:** The Government usually adopts a high trust approach during an emergency which enables support to be delivered as quickly as possible, but also has a greater risk of fraud and error.
- **Increased financial flow:** Emergency relief and recovery situations often lead to an increase in funding to the affected area which can create more opportunity for fraud.
- **Lack of verification:** The urgency of a recovery situation can make it difficult to verify the legitimacy of requests for assistance. Depending on the emergency, documents that would often be relied upon for verification may have been damaged or are unable to be accessed. For example, if a property has been flooded identity documents or bank statements may have been destroyed or lost; or the owner might not be able to retrieve them from the property. Any flexibility in verification scrutiny can make it easier for fraudsters to be successful with fraudulent applications.
- **Urgency and distraction:** In an emergency, people will often be dealing with multiple developing situations and can therefore be more focussed on other immediate concerns. This may make them less vigilant or cautious and can create opportunities for fraudsters to exploit the situation and fraudulent activities to go unnoticed.
- **Disrupted systems:** Emergencies can disrupt normal systems and processes, including those which track or hold valuable sources of information. This disruption can create gaps that fraudsters exploit.
- **Opportunistic behaviour:** Some individuals may also use emergency situations for purely opportunistic reasons to commit fraud by taking advantage of the disruption.



5 Principle 2: Integrate Fraud Control Resources Into Policy Design and Processes

By integrating personnel and training employees, organisations can better anticipate and identify fraudulent actions, reducing the chances of fraud occurring or slipping through unnoticed.

5.1 Integrate Fraud Control Resources

When developing emergency management policies and processes, it is important to have someone analyse the policies and processes from a fraud risk perspective as they are developed.

During emergencies, policies and processes can shift quickly and the teams developing them may not have the capacity to actively identify and record fraud risks as they occur. This is why it is an advantage to have dedicated counter fraud capability during emergencies.

If there are skilled and experienced fraud personnel available within the organisation it is important to involve them from the outset of policy and process design. If there is not a dedicated counter fraud specialist, someone from the risk or assurance team can also be a valuable resource and should also be involved from the outset.

Counter fraud personnel are skilled and experienced at understanding and assessing fraud risks and developing effective countermeasures. These skills may be found in a single person, or there may be a few individuals with skills and experience in different types of risk or counter fraud roles. It is important that the person in this role is able to identify fraud vulnerabilities (by carrying out a fraud risk assessment), document them, and communicate them to the relevant people.

The fraud control role can be a passive one, which observes the policy and process development meetings, or a more active role, which facilitates an understanding of the fraud risks with the policy and delivery leads and teams. The approach taken is dependent on how the team is operating and the best role the fraud control resource can serve. What is important in this role is that those responsible for developing policies and processes during this time are made aware of the fraud schemes that are likely to occur during the relief and recovery phase.

The Counter Fraud Centre can support existing fraud control staff or offer guidance to organisations that might lack fraud control capability. Get in touch with the team at counterfraud@sfo.govt.nz

5.2 Equip Employees to Prevent and Detect Fraud

Employee awareness of fraud is a key control in the delivery of emergency relief and recovery funding. The Association of Certified Fraud Examiners Report to the Nations (2024) has found that fraud awareness is one of the most effective tools for fraud prevention, with more than half of fraud cases being detected by employee tip-offs.⁴ Fraud awareness and education is therefore an important part of encouraging employees to identify and report suspicious behaviours.⁵

Training employees to be aware of fraud and how to report it, as well as ensuring that they receive regular messaging on fraud awareness, can help to improve this key control and increase the likelihood that fraud is deterred and detected.

Outlined below are some of the common types of fraud that can occur during an emergency response and recovery process:

- **Misappropriation of funds:** Diverting relief funds for personal gain rather than using them for the intended relief efforts.
- **Double-Dipping:** Applying for emergency relief funding from multiple sources by providing false information or misrepresenting their needs.
- **False claims and documentation:** Submitting false claims or fraudulent documentation to obtain emergency funds that the person is not entitled to.
- **Identity Theft:** Stealing the identity of others to access emergency relief funding in their name.
- **Corruption:** Exchanging bribes or kickbacks in return for access to emergency relief resources or contracts.
- **Procurement fraud:** Fraudulent procurement practices such as awarding contracts to fictitious or unqualified suppliers.
- **Cyberattacks and Phishing:** Relief organisations may be targeted by cybercriminals who use phishing emails or other cyberattacks to gain unauthorised access to emergency relief funding.

⁴ Association of Certified Fraud Examiners Report to the Nations, "Report to the Nations" (2024) page 4.

⁵ For help with this, check out our [Counter Fraud Messaging guide](#).



6 Principle 3: Implement Low Friction Countermeasures

Low friction fraud countermeasures aim to detect and prevent fraud without creating significant delays or administrative burdens. These measures strike a balance between fraud risk management and maintaining the speed and efficiency of response efforts.

These measures, though essential for managing fraud during an emergency response, can be integrated into routine operations, ensuring that they are already in place when an emergency arises. In particular, using existing processes and delivery models will help to implement effective countermeasures at pace.

6.1 Coordinated Response to Fraud

A coordinated response is about having a well-organised plan to prevent and deal with fraud. It involves working together with responsible agencies and community groups to make thoughtful decisions at every step – from setting up the system, reviewing and approving the applications, to post-event assurance. A coordinated approach will help ensure decisions are made following best practice under challenging circumstances. It can also help reduce opportunities for fraud and protect the integrity of the overall response.

Governance, Accountability and Oversight

Ensuring there is good governance, accountability and oversight over response processes can help increase transparency and reduce opportunities for fraud. Organisations may need to streamline their standard decision-making and governance processes to respond more swiftly to emergencies, while at the same time preserving oversight and transparency.

Emergency relief and recovery programmes are typically delivered at pace and there are ever-changing requirements for responses. As a result, there is often more difficulty involved to ensure robust governance measures. Organisations may need to quickly on-board new staff or redeploy staff to help with the response. This can disrupt established reporting lines and oversight, so it is important that any governance arrangements are adaptable to the new conditions.

It is crucial that organisations set a clear tone from the outset on how fraud risks will be managed. Good governance includes designating an individual to manage fraud risks and vulnerabilities during an emergency. Project reporting requirements and governance arrangements should also be put in place to encourage transparency and accountability for project outcomes.

Fraud Reporting Line

A fraud reporting line provides a mechanism for individuals to report issues or concerns regarding suspicious behaviours in relation to the response efforts. This is an important way to help identify potentially fraudulent activities and provides a centralised point for collecting reports of suspect fraud. For maximum effectiveness, the reporting process should be clearly communicated and handled confidentially, encouraging employees, and individuals or businesses in the community to come forward with their concerns. Additionally, it is beneficial to specify the type of information needed when making a report to ensure that it contains sufficient details for appropriate action.

Work With Well-Established and Trusted Partners

When working with other organisations and businesses to deliver emergency response and relief funding, there is often limited time to conduct thorough upfront due diligence or fit-for-purpose checks on those groups. This is due to the urgency of providing immediate support to those in need, and can lead to a higher risk of fraud as an organisation must weigh up the importance of timely support versus the need for robust verification of the information they are being provided.

Working with partners such as other government entities, reputable non-government organisations, and established businesses to deliver services can reduce this risk. Where an organisation has previously been vetted to carry out work it can help reduce fraud risks by eliminating the need for prior due diligence, as they are already a trusted supplier.

6.2 Application Processes

Clarifying the application process, eligibility criteria, and an applicant's obligations when receiving emergency relief and recovery funding can help to reduce opportunities for fraud and misuse. It also makes it easier to identify and address missing or inconsistent information.

Clear and Comprehensive Eligibility Criteria

Eligibility criteria should be well set out and provide sufficient guidance for applicants, so they clearly understand whether they are eligible for funding before they begin the application process.

Without clear eligibility criteria it can lead to a recipient unintentionally failing to meet their obligations or make it difficult to demonstrate that they have met the criteria. Applicants should be able to understand what evidence may be required as part of any application or post-assurance process.

Fraud Clauses

Fraud clauses are provisions included in contracts, agreements, or legal documents designed to address and mitigate the risk of fraud. They outline the consequences should fraudulent activity be suspected or detected.

Given the high volume of support claims that are made during emergency relief and recovery situations, the manual verification of them can be impractical, especially where there is a need for rapid distribution of funding. Fraud clauses can therefore be a useful tool to ensure that any funding provided that is later found to not fit the eligibility criteria can be recovered by the organisation.

It is important that applicants are required to ensure the accuracy and validity of any information they submit. This can be helped by incorporating any fraud clauses into initial disclaimers or contracts, which applicants are required to sign, and should be prominently displayed and accompanied by a consent box. They should also clearly outline the consequences of providing false or inaccurate information.

By indicating that organisations may pursue civil or criminal actions in cases of suspected fraud, these clauses can also act as a deterrent for opportunistic fraudsters. Because fraud clauses have legal implications, it is crucial to seek legal advice before including them to ensure they are enforceable.

Claw Back Arrangements

Recovery or claw back arrangements allow an organisation to seek repayment if a grant or payment is made in error. These arrangements can also be used if the funds were not distributed or used according to the specified requirements. This might be because the recipient was later found not to have met the eligibility requirements, or they could not prove that the funding was used for the stated purpose.

Claw back arrangements are particularly relevant in emergency relief and recovery situations, where funding might be distributed in error due to the rapid timeframes that often prevent thorough upfront verification checks. These arrangements ensure that if mistakes occur, funds can be recovered after distribution.

These clauses can be incorporated into applications, disclaimers, and contracts, or established through legislation. Enforcing such clauses by seizing assets and recovering funds paid due to fraud acts as a powerful deterrent against fraudulent activities.

Publication of Recipient Information

One particularly effective measure, highlighted during the distribution of the COVID-19 wage subsidy scheme, was the publication of businesses who received subsidy payments including the employer's name and the amount of subsidy funding received. Making this information publicly available, provided greater levels of transparency and an additional level of scrutiny of payments.

When inaccurate information was identified, the public could report concerns regarding an applicant's eligibility for payments. They were also able to flag cases where employers failed to pass on subsidy payments to employees, as required.

Parameters or Limits

To expedite claim processing during an emergency, an organisation can establish maximum payment limits or set application thresholds to pinpoint where additional scrutiny is necessary. Setting specific parameters and limits allows organisation to expedite applications that fall under a particular threshold while applying additional scrutiny to applications that are deemed to fall outside that accepted threshold of risk.

6.3 Reviewing, Approving and Processing Applications

A streamlined application process enhances the effectiveness of fraud risk management by ensuring resources are applied fairly and efficiently.

Payment Processes With Oversight

Distribution of emergency funding can often mean that there is an influx of applications. To process these applications in a timely manner organisations must sometimes on-board or redeploy employees.

Because of the greater number of employees involved in the reviewing of applications, it can also increase the risk of fraud occurring. Staff who have not had sufficient training or experience in reviewing applications may overlook fraudulent activities.

Where there is any disruption of established reporting lines it can lead to a similar disruption in effective oversight and accountability. Where possible, it is important that access to payment processes is restricted to only essential personnel and that there is robust oversight of activities. Segregation of duties between the various stages of reviewing and approving applications can also help to reduce coercion and the concealment of fraudulent activity.

Leaders involved in the application process should ensure that they are regularly communicating with staff about how to identify red flags, discuss fraud risks and how to escalate issues during periods where there is a disruption of normal workflows.

Principle Four in this guide also provides a detailed exploration of the concept of post-payment verification.

Collecting and Retaining Information

Public organisations are accountable to Parliament for how they make decisions about public spending. Reasons for providing funding should be clearly explained and well documented.

Robust record-keeping to support the rationale behind decision-making and processes followed is particularly important during emergency situations. In addition, having a reliable dataset that can be referred to as part of post-event assurance activities is particularly valuable to ensure the accuracy and reliability of claims.

Data analytics can be used to identify potential fraud or high-risk areas. This can include using data to:

- build a holistic view of applicant behaviour across different disaster relief and recovery payment types
- validate information captured at application stage
- identify applications containing identical information.

Leverage Employees' Existing Knowledge in the Application Processing

In some instances, those working within a public sector organisation may have already had previous dealings with individuals and/or businesses applying for emergency relief and recovery funding. These employees can be valuable resources for detecting discrepancies and inconsistencies in the information provided by applicants.

Where possible it can be beneficial to use the information already held about applicants when processing applications for emergency funding. This is especially important when there is a short timeframe to distribute funding. By leveraging existing knowledge and data, it can help verify the accuracy of claims and be used as a form of data matching to reduce the risk of fraudulent applications.

There may also be times when employees hold valuable information outside of the skillset for which they are employed. For example, where flooding occurs and recovery funding is available to only those who are specifically impacted, employees who have particular knowledge about geographic areas and features can be leveraged to verify the accuracy of claims.

Data Matching

Data matching strengthens the integrity of verification processes during emergency relief and response situations. It helps to reduce the risk of fraudulent activity occurring by using previously verified information

Examples of data matching include:

- **Use of publicly available data to identify and verify businesses.**

You can use the [Companies Register](#), [New Zealand Business Number Register](#), [Charities Register](#) and the [Charitable Trusts Register](#) to access open-source data to identify and verify business details.

- **Information Matching is a programme run by the Department of Internal Affairs.⁶**

It is the comparison of 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.

- **Data or Information Sharing Agreements between organisations.⁷**

This can speed up the verification of information to confirm eligibility for emergency support. Effective data sharing can be a powerful tool for preventing and detecting fraud.

- **Use existing data sets.**

Where possible, compare incoming data with existing internal data sets to perform seamless upfront checks or conduct post-event assurance activities.

⁶ <https://www.dia.govt.nz/Legal-Privacy-Information-Matching>

⁷ <https://privacy.org.nz/tools/knowledge-base/view/168>



7 Principle 4: Carry Out Post-Event Assurance

Post-event assurance is where an organisation carries out checks for any instances of fraud that may have occurred during the distribution of relief and recovery funding. The need for rapid distribution of emergency funding often means that the time available to implement preventative countermeasures is limited. Because of this, the post-event assurance process is important to help detect fraudulent or erroneous claims for support.

Organisations should use the fraud risk assessment created during the policy and process design (see [section 5](#)), to carry out post-event assurance activities. It is crucial to conduct timely post-event activities to verify whether the anticipated fraud risks materialised.

It is also important during the planning stages of emergency relief and recovery funding situations that resources are allocated for post-event assurance activities. Thought should be given to the appropriate level of post-event assurance. Any assurance activity is better than none.


When announcing emergency payments or services, highlighting that there will be checks undertaken after the payments have been made, can act as a deterrent to would-be fraudsters. The insights gained from these assurance activities should also be used to refine existing processes. This can help to reduce incidences of fraud in the event of a future emergency occurring.

7.1 Types of post-event assurance

The type of post-event assurance that an organisation chooses will depend on the fraud risks relevant to the emergency relief and recovery funding.

Examples of post-event assurance activities include:

- **Verifying eligibility:** Confirm that the claimant met the eligibility criteria by cross-checking supporting documentation and information. This process typically involves a more thorough review than might have been possible during the initial distribution of emergency funding. It might include verifying claims about circumstance or geographic location, that may be different from the actual situation.
- **Invoice verification:** Verify whether a provider delivered the products or services for which they have provided an invoice.
- **Duplicate payments:** Duplicate payments can occur due to administrative errors or fraudulent activities. Checking for instances where this may have occurred is a reliable post-event check.

- 
- **Pattern recognition:** Look for patterns of claims which might be an indicator of possible administrative error or fraud. For example: several claims from different individuals or organisations but which use the same contact details and/or bank account number can be an indicator of suspicious activity.

After a time-critical emergency management situation has ended, organisations should review lessons learned regarding fraud and how it was controlled. Insights from reviews can enhance future emergency response programmes and be used to adjust current processes for less urgent scenarios.



8 Principle 5: Be Mindful of the Shift Into Longer-Term Services

Emergency relief and recovery funding can also cover longer-term relief efforts. It might also include infrastructure rebuild projects, or ongoing support payments to affected individuals.

Longer-term support led by the same organisation or team that led the emergency response creates a risk that short-term processes continue longer than initially intended. This can increase the fraud risk as short-term systems and processes may not have the same level of controls. This may then carry on into the longer-term provision of less time pressured emergency response situations.

Those leading relief efforts should recognise the shift to longer-term service provision and take the opportunity to revisit and assess the associated fraud risks and countermeasures. If the low-friction countermeasures that were appropriate during the initial response are continued without adjustment, fraudsters might exploit these opportunities, which could otherwise be prevented.



9 Examples of Fraud in Emergency Management

The following cases provide examples of the types of fraud that can occur following the distribution of emergency relief and response funding:

Case 1: Man jailed for almost \$200,000 wage subsidy fraud

<https://www.msd.govt.nz/about-msd-and-our-work/work-programmes/wage-subsidy-integrity/2023/jail-for-almost-200000-wage-subsidy-fraud.html>

Case 2: Fraudster used doctored license to obtain wage subsidy

<https://www.msd.govt.nz/about-msd-and-our-work/work-programmes/wage-subsidy-integrity/2023/fraudster-used-doctored-license-to-obtain-wage-subsidy.html>



**Counter
Fraud Centre**
TAUĀRAI HARA TĀWARE

Content from the following sources has been used in the preparation of this guide:

Managing public funding in an emergency response or recovery – Observations from our work.
Office of the Auditor General, <https://oag.parliament.nz/2023/emergency-funding>

Lessons learned: tackling fraud and protecting propriety in government spending during an emergency
Cabinet Office and HM Treasury, [Lessons learned: tackling fraud and protecting propriety in government spending during an emergency \(nao.org.uk\)](https://nao.org.uk/publications/lessons-learned-tackling-fraud-and-protecting-propriety-in-government-spending-during-an-emergency)

Fraud in Emergency Management and Recovery Principles for Effective Fraud Control
International Public Sector Fraud Forum, https://assets.publishing.service.gov.uk/media/5e3d4f7d40f0b60917d6591e/Fraud_in_Emergency_Management_and_Recovery_10Feb.pdf

© Commonwealth of Australia 2023 CC BY Commonwealth of Australia 2023.
Where relevant, content has been adapted for the New Zealand context.



SFO

SERIOUS FRAUD OFFICE
TE TARI HARA TĀWARE

Te Kāwanatanga o Aotearoa
New Zealand Government