International Public Sector Fraud Forum
Bringing countries together to fight public sector fraud

International Public Sector Fraud Forum

Fraud in Emergency Management and Recovery

Principles for Effective Fraud Control

February 2020

Cabinet Office

Commonwealth Fraud Prevention Centre

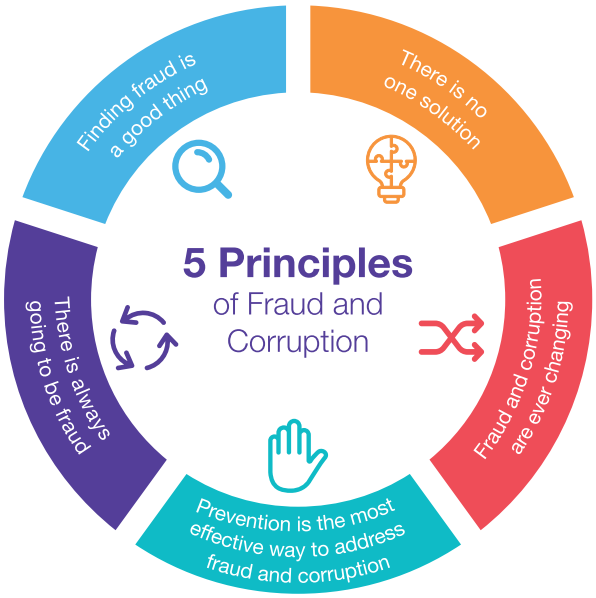
Produced in collaboration with the Cabinet Office and the Commonwealth Fraud Prevention Centre.

Contents

The International Public Sector Fraud Forum

The International Public Sector Fraud Forum (IPSFF) currently 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.

The Forum has established 5 principles for public sector fraud.



1. There is always going to be fraud

It is a fact that some individuals will look to make gains where there is opportunity, and organisations need robust processes in place to prevent, detect and respond to fraud and corruption.

2. Finding fraud is a good thing

If you don't find fraud you can't fight it. This requires a change in perspective so the identification of fraud is viewed as a positive and proactive achievement.

3. There is no one solution

Addressing fraud needs a holistic response incorporating detection, prevention and redress, underpinned by a strong understanding of risk. It also requires cooperation between organisations under a spirit of collaboration.

4. Fraud and corruption are ever changing

Fraud, and counter fraud practices, evolve very quickly and organisations must be agile and change their approach to deal with these evolutions.

5. Prevention is the most effective way to address fraud and corruption

Preventing fraud through effective counter fraud practices reduces the loss and reputational damage. It also requires less resources than an approach focused on detection and recovery.

Foreword

Mark Cheeseman
Deputy Director Public Sector Fraud,
UK Cabinet Office

In times of emergency or disaster recovery situations, it is important that government can get funding to where it is needed as quickly as possible. This includes providing support and services to those in need and rebuilding communities and infrastructure. Fraud can undermine these efforts if it is not controlled.

Sadly, the provision of emergency relief and services has an inherently high risk of fraud, and is a prime target for those seeking to make gain at the expense of others. There are numerous examples from across the world of people taking advantage at times of need.

Those leading the creation and administration of this support should be aware of the threat posed by fraud and be able to make conscious decisions on which risks are to be tolerated. The only way to make an effective decision on what tolerance there may be for fraud is to understand how the emergency management situation may be defrauded.

The members of the IPSFF recognise the importance of effective emergency management and the sad reality is that fraud is often an issue in these circumstances. Through providing insight from our leading practises on fraud control in emergency management, we hope to empower public bodies to better manage fraud in emergency contexts and, as a result, enable essential emergency management to be more effective.

In these environments, the largest failure would be to not get support to those who need it. It is not a failure for some fraud to happen – a certain level of fraud is inevitable and likely unpreventable due to the time-critical nature of delivery. This loss will have to be accepted.

What would be a failure is for fraud to happen in an uncontrolled manner, with the responsible leaders unaware. When fraud happens in an uncontrolled manner, it can quickly become endemic. This in turn can have significant impacts: increasing the cost of emergency management and reducing the resources available to government to manage the issue, leading to further suffering for disaster victims. It can also erode the good will of the community and undermine confidence in the government's response.

To stop this from happening, those leading responses should have resources in place to understand how fraud could happen, and take proportional action to look for it in the system.

This guidance is designed to help those leading and working on the administration of emergency management situations to understand the practical way to deal with fraud and reduce risk. It is designed for those in the public sector. However, it is equally relevant to those in other sectors.

In this guidance, the term fraud is used to cover economic crime more generally (i.e. individuals or groups being dishonest to make gain). This can include loss as a result of corruption, where corruption leads to fraud.

The Principles of Fraud Control in Emergency Management

The following are the principles of effectively controlling the levels of fraud in emergency management contexts.

Accept that there is an inherently high risk of fraud, and it is very likely to happen.

Integrate fraud control resources (personnel) into the policy and process design to **build awareness of fraud risks**

The business and fraud control should work together to **implement low friction counter-measures** to prevent fraud risk where possible

Carry out **targeted post-event assurance** to look for fraud, ensuring access to fraud investigation resource

Be **mindful of the shift** from emergency payments **into longer term services** and revisit the control framework – especially where large sums are invested

In doing all of this we must be mindful of the fundamental purpose of the emergency context – **getting payments and services to those in need is the priority.**

What is Emergency Management?

Emergency management is the organisation and management of the resources and responsibilities for dealing with all humanitarian aspects of emergencies (preparedness, response, mitigation and recovery). The aim is to reduce the harmful effects of all hazards, including disasters. In some environments this is can be called disaster or crisis management.

In recent years there have been a number of high profile emergency management responses following crises. These can be after natural disasters, such as floods, hurricanes and fires, or after man-made disasters, following events such as war or terrorist attacks.

Commentary indicates that the frequency of these instances seems to be increasing, and as such, the Public sector is increasingly drawing on emergency management as a discipline. At the same time, the effectiveness of government and humanitarian organisation (both individually and together) responses increases. Effectively managing fraud and corruption in these environments is an important part of increasing the effectiveness of emergency management, and the confidence in government and humanitarian organisations in the delivery of it.

This guidance focuses on the time-critical aspects of emergency management (preparedness, response, mitigation and recovery) rather than the longer-term efforts to manage potential emergencies.

The principles detailed in this guidance can also be applied to any other area where government, or any organisation, needs to move to implement services quickly due to the circumstances they are in. For instance, when the United Kingdom was preparing to leave the European Union and time critical action was needed to prepare effectively, these principles were relevant.

Why does Emergency Management have an inherently high risk of fraud and corruption?

In times of crisis it is important that government can get public money to where it is needed quickly and efficiently. Where there are individuals, communities or services in need of urgent funding, services or supplies, the priority must be to ensure that it reaches them to enable the crisis to be managed and those impacted to be supported.

Crises can bring communities together and bring the best out in people, giving their time and money to support those in need. However, sadly crises also attract those with more negative motives.

There are numerous examples of where fraudsters use emergency situations to make gain, either through receiving services that they are not entitled to, or through acting fraudulently in the delivery of services to support affected communities. There can also be significant fraud from those purporting to help affected communities where they are not. Examples of emergency management fraud are included in **Annex A.**

In emergency situations, policies, systems and processes have to be put in place rapidly. This limits the time that is available for reflection on what the criteria are for payments to be made or services to be delivered. It also limits the time for processes to be clearly defined, systematically recorded, and analysed.

Inevitably, emergency payments have to be made quickly. This means the appetite for up-front controls to check eligibility for a payment (which may delay those payments) is low.

Often, those in emergency situations have less evidence of their circumstances and how they meet the criteria for payments or services. As such, checks are less easy to perform at the pace that is necessary, and sometimes the usual checks cannot be done. For example, an individual whose property has been damaged or destroyed may have lost the documents that they would use to prove their identity.

As a result of the above factors, the threat and risk of vulnerabilities to fraud are inherently much higher in emergency management. This should be acknowledged by the business, those leading the administration of emergency management, and by those assisting in fraud control. There should also be an acceptance that the priority is to get funding to affected communities and services and this will inherently mean a high likelihood of fraud in the system.

It is worth noting that the nature of the emergency management situation can have a significant impact on the types of fraud that arise and the impacts of these frauds. For instance, in a crisis involving fire, debris may be difficult to dispose of – requiring complex processes. In these processes, corners may be cut, which can have financial and public health impacts. Also, where a disaster has an impact on property it can be easier to mislead in some circumstances (such as storms) in comparison to others (such as floods and fires). Those working in emergency management situations should be mindful of the unique opportunities for fraudsters that may be relevant to the situation they are in.

Why should we care about fraud in Emergency Management?

When the priority in emergency management situations is to provide support and services to individuals, communities and areas in need as swiftly as possible, it could be asked why fraud and corruption should be considered at all.

Financial Impacts

Where fraud and corruption happen, there are many impacts. Most obviously, there is a financial impact; redirecting funds away from activity that would support the emergency and the communities. This can increase the cost of emergency management, and lead to less support and services going to those affected by the disaster or crisis.

Fraud in the rebuilding process following any disaster can also increase the cost of rebuilding and make it take longer – having a knock-on impact on the communities involved. emergency management consumes significant public sector funding. For example, the government of the United Kingdom's response to the Grenfell Tower disaster cost around £250m, and the United States response to the impact of Hurricane Katrina cost around $110bn.

Human Impacts

There can also be a human cost. Fraud and corruption can lead to an increased level of emotional and psychological impact on the victims. Fraud in emergency management can be against the funding and services allocated or created to deal with the situation. However, fraud can also be against communities or victims themselves - for instance, through fake fund-raisers. Where the public sector is responsible for leading the emergency management, there is an expectation that the government will play a role in controlling this broader fraud.

Public Trust

Fraud and corruption undermine the public's trust in government. In emergency management situations, trust between government and the community is important as it means communication and action can happen effectively and efficiently. At the mildest, a breakdown in trust can lead to a reduced confidence in the government and those responsible for leading the response. At the most extreme, it could lead to destabalisation and a resulting intensification of the emergency situation.

While fraud cannot be eradicated from emergency management it can be controlled and limited, increasing the community's confidence in the response and maximising the funding that goes where it is needed. Uncontrolled fraud and corruption can become endemic. A high level of fraud in an emergency management programme can completely undermine the community's perception of the effectiveness of the response.

Accept an inherently high risk of fraud | Integrate fraud control resources and build awareness of fraud risks | Implement low friction counter-measures | Carry out targeted post-event assurance | Be mindful of the shift into more longer term services

Accept that there is an inherently high risk of fraud, and it is very likely to happen.

Page ten details why emergency management situations are at an inherently high risk of fraud. **Annex A** contains some examples of fraud and corruption in emergency management.

It is important that those working to develop responses accept that there is a high risk of fraud and that it is necessary to tolerate some degree of fraud within these payments and services.

The failure is not in fraud happening. It is in not having arrangements in place to understand how it could happen, and then looking for it in the system. Fraud is a hidden crime and is best found through conscious detection activity.

Integrate fraud control resources (personnel) into the policy and process design to **build awareness of fraud risks**

When policy and delivery areas are developing emergency management policies and processes, there should be skilled and experienced fraud resources (personnel) associated or embedded to analyse the policies and processes as they are developed. Their role is to identify how the system could be defrauded (by carrying out a fraud risk assessment), to record this, and to communicate it to the key responsible leads. It should be part of the role of the leader of the emergency management activity to ensure effective fraud control resource is identified and embedded.

Policies and processes can often shift quickly in these circumstances and the teams developing them may not have the capacity to actively record fraud risks as they evolve. This is why it is an advantage to embed the resource.

The integrated fraud resource should ideally be fraud control resource (as opposed to fraud investigation resource). Fraud control resources are skilled and experienced at understanding and assessing fraud risk and developing effective countermeasures. These skills may be found in a single person, or there may be separate individuals with particular skills and experience in different types of risk or counter fraud measures. While audit, legal and finance professionals can make effective counter fraud resources, they are not usually trained in these disciplines.

This can be a passive role, that observe 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.

The resource should build a fraud risk assessment, which will detail how the policies and processes could be defrauded. For more information on what an effective fraud risk assessment should look like, refer to **Annex B.**

Without a fraud risk assessment, those responsible for emergency management will have no awareness of how the response could suffer from fraud or corruption. They will not be able to implement effective counter fraud measures or build an awareness in the system of fraud. As such, the overall risk and likelihood of fraud and corruption would be much higher.

Accept an inherently high risk of fraud | Integrate fraud control resources and build awareness of fraud risks | Implement low friction counter-measures | Carry out targeted post-event assurance | Be mindful of the shift into more longer term services

The business and fraud control should work together to **implement low friction counter-measures** to prevent fraud risk where possible

Once they understand some of the risks of fraud and corruption, the fraud control resources (personnel) should actively support the policy and delivery teams by suggesting key countermeasures that could be used to reduce some of the most significant risks.

In an emergency management environment, it is important that these counter-measures are low friction, so they do not delay any urgent payments or services. Examples of potential counter-measures are included in **Annex C.** The ideal response is to include some, low friction, up front controls that significantly reduce fraud risk without delaying payments or services.

The most effective way of implementing counter-measures at pace is to use existing processes and delivery models. However, this may not always be possible. Modelling policies and criteria for the delivery of support or services on things that are already established and tested can reduce the fraud risk, or at the least enable the risks to be more efficiently and easily understood.

Using established providers, where possible, can often be a lower risk option than using new, unestablished and untested providers, on which the government has less information. However, it should be remembered that it is individuals that commit fraud - not organisations. It is not possible to eliminate the risk of fraud using established and ‘trusted’ providers.

As some of the usual up front, preventative controls (such as document or evidence checks) may be difficult to implement in emergency management situations, particular consideration should be given to what detective controls can be introduced to make the fraud or corruption that does occur more apparent.

Where it is not feasible to implement controls to mitigate established vulnerabilities (either due to the urgent payments/services needed or the investment needed to establish the control) the fraud control resource should be active in recording the risks that result so they can be considered later.

Carry out **targeted post-event assurance** to look for fraud, ensuring access to fraud investigation resource

The extent to which up front, preventative, counter-measures can be implemented will be limited. As such, it is important that post event activity is undertaken (in as timely a fashion as possible) to establish whether the fraud risks established and understood came to pass. Using the fraud risk assessment created during policy and process design, the business should carry out post-event assurance work to check for instances of fraud.

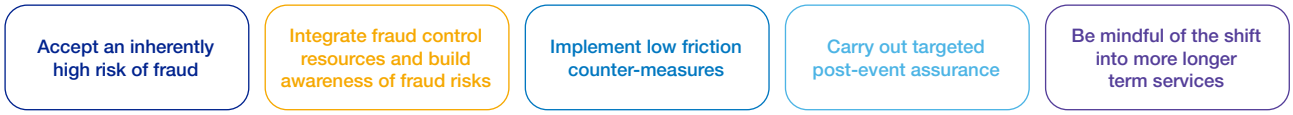
It is important, during planning, that resources are agreed and put aside to deliver this. Post-event assurance can be done on a variety of scales. It could be the allocation of time from an audit plan, expanded or reprioritised activity in an already established resource (for instance the Inspector General's departments in the United States), or the investment in new, capable compliance resources. Thought should be given to the appropriate level of post event assurance. It should be remembered that any post-event assurance activity looking for fraud is better than none. Consideration should be given to cost of post-event assurance in up front scoping of the emergency response.

It is possible to put in place larger structures that can be relied on by a number of emergency management situations. In the United States, in 2005, the government created the National Centre for Disaster Fraud to improve the detection, prevention, investigation and prosecution of fraud associated with disasters. It also acts as an advocate for the victims and the impact that fraud has on them.

From 2005 to 2019, the NCDF had received over 95,000 complaints relating to disaster fraud. In relation to Hurricane Katrina alone, it prosecuted 1,300 disaster fraud cases.

Post-event assurance consists of considering the fraud risk assessment and reviewing a sample of payments and services, in light of the risks, to see if any instances of fraud can be identified. The focus should be on actively looking for fraud in the system, rather than checking whether controls have been undertaken successfully. This is especially relevant in emergency management situations where controls and counter-measures are likely to be less extensive. Examples of post-event assurance are:

- If the risk is that individuals claim to have different circumstances to their actual ones (for example, being someone else or living somewhere else), the circumstances are checked more thoroughly than they were able to be in the emergency management situation;
- If the risk is that a provider of services makes claims for services they have not delivered or inflates their fees, their claims and activity undertaken are reviewed more thoroughly retrospectively.



In addition to securing or putting aside resource for post-event assurance, it is important that there is, at least, access to fraud investigation resources. These may not be necessary, but if potential fraud is identified they will be.

Fraud investigation is an increasingly complex and technical activity. Investigations into potential fraud or corruption should not be given to generalists, but to trained and experienced fraud investigators.

When announcing emergency payments or services, highlighting that there will be post-event assurance checking can act as a deterrent to would be fraudsters.

Be **mindful of the shift** from emergency payments **into longer term services** and revisit the control framework – especially where large sums are invested

Emergency management covers both the management of emergency situations and longer term emergency management such as the building of preventative policies and measures and the rebuilding of communities and infrastructures that have been damaged.

The principles in this guidance are especially relevant to the management of an emergency/crisis or strongly time pressured situation. There often comes a point when the initial time-pressured response comes to an end and more systematic investment starts for longer term services and support (for example, moving into the rebuilding phase).

If this is led by the same organisation or team that led the emergency response, there is a risk that the short term processes and culture built by the team developing the polices and processes can last longer than is necessary for dealing with the situation they are managing. This can unnecessarily increase the risk of fraud and corruption in these less time pressured emergency management situations.

Those leading emergency management should aim to be aware of this shift and the opportunity to revisit the fraud risks and fraud controls.

It is essential that fraud risk is reconsidered during this period of transition. If the low-friction preventative fraud countermeasures that were appropriate during the initial response are maintained, fraudsters are likely to take advantage of these, which could be prevented.

Fraud and the Emergency Management Cycle

Emergency management is not a one off event. The discipline covers the broader spectrum of preparedness, response, mitigation and recovery. Often, government has to react to a disaster or a crisis quickly. However, the government will have an overall emergency management/civil contingencies system, which includes preparedness for crises and mitigations to reduce their likelihood or impact.

Whilst this guidance focuses on the time critical aspects of emergency management, the threats and risks of fraud should be considered throughout the whole lifecycle of broader emergency management.

Preparedness

Part of emergency management is, before emergencies occur, considering what places or circumstances are at risk of emergency and what mitigations are in place to deal with any emergencies effectively and reduce their impact. As part of this activity the risk of fraud should be significantly reduced by activities such as vetting suppliers and creating preferred supplier lists in key areas where there is a risk of an emergency management situation. By considering the risk of fraud in these, less time critical, environments more effective controls and counter-measures can be established, which can then be used.

Lessons Learned

In addition, once any, time critical, emergency management situation has been concluded organisations, and government as a whole, should take the opportunity to consider any lessons learned on fraud and how it was controlled. This can then be built into future emergency management. The post event assurance (principle 4) undertaken is a key tool for this process, providing the evidence of where the policies, processes and services have worked as intended and where they have been taken advantage of.

Departure from Established Controls

Over time, as emergency management processes and policies become more and more proactive and established, it may be that the conversation changes from what controls should be included to what established controls may need to be removed to ensure essential services and support gets to those in need. In this case, overall emergency management processes could have ‘minimum standards’ for controls (built through experience and reflection as part of the wider emergency management practice). Effectively, organisations would be moving away from the minimum standard to expedite the response. In these circumstances, the principles still hold. The fraud resource should be understanding the increase in fraud risk that result from the departure from any ‘minimum standard’ as part of their wider analysis of fraud risk.

Annex **A**

Annex A – Examples of Fraud in Emergency Management

The following annex provides some examples of the types of fraud that can happen around emergency management.

A Mississippi man submitted a **fraudulent claim to BP's Gulf Coast Claims Facility for lost earnings and profits,** which he claimed **were incurred as a result of the oil spill which led to loss of employment.** An investigation revealed that the documents and claims he submitted were fraudulent, the named businesses did not exist, and he never worked at any such company. As a result of the man's fraudulent scheme, a check was mailed to him in the amount of $23,541.

→ www.justice.gov/usao-sdms/pr/gulfport-man-sentenced-deepwater-horizon-oil-spill-fraud

---

Shortly after Hurricane Katrina, Scott Benson and Chris Armstrong masqueraded as Salvation Army workers to **con more than 2,500 police officers, firefighters, sheriff's deputies and FBI agents into disclosing personal information.** The men told officers that they were eligible for debit vouchers worth $5,000 in a program sponsored by media company Viacom. The men were charged with false impersonation and conspiracy to commit identity theft.

→ www.insurancejournal.com/news/southcentral/2005/09/22/59924.htm

---

A South Florida man collected $23,244 in Federal emergency management Agency aid after Hurricane Frances in 2004 by **claiming that the boat on which he lived was damaged.** His primary residence was actually an apartment. He was among 26 other South Florida residents to have been charged with filing false Hurricane Frances claims.

→ www.fraud-magazine.com/article.aspx?id=4294967697

A Federal emergency management Agency (FEMA) inspector was arrested on charges of accepting kickbacks for approving false hurricane damage claims.

→ www.acfe.com/article aspx?id=429496769

In February 2008, a federal grand jury in the Southern District of Texas indicted a man on two counts of wire fraud relating to his alleged operation of a fraudulent investment scheme. Beginning in 2006, the defendant allegedly falsely told investors he was using their money to purchase and refurbish Federal emergency management Agency (FEMA) trailers but failed to ever purchase the trailers and failed to return the investors' money.

→ www.govtech.com/em/disaster/Hurricane-Katrina-Fraud-Task.html

---

The 1972 earthquake in Managua, Nicaragua, led to large scale government corruption in relief and reconstruction. This contributed to Sandinista rebels capitalising politically and opening a military campaign in 1975.

→ www.odi.org/sites/odi.org.uk/files/odi-assets/publications-opinion-files/8228.pdf

---

On June 6, 2008, a federal grand jury in the Middle District of Alabama indicted a former FEMA manager for embezzlement of a trailer intended for victims of Hurricanes Katrina and Rita. The indictment alleges that the defendant, while the manager of an emergency housing unit, embezzled a 39-foot Cherokee Travel Trailer and his government vehicle, to which he had access by virtue of his management position. It also charges him with attempting to corruptly influence the ongoing investigation against him in the Middle District of Alabama.

→ www.justice.gov/archive/opa/pr/2008/October/08-crm-877.html

---

Following disasters, it is possible that damaged assets, such as vehicles, may be purchased as salvage and then restored and transported to a different location. They could then be resold concealing any problems (such as water damage to electronics and computers systems in vehicles as a result of flood damage). These problems may not be visible at first but may cause problems later

→ www.nw3c.org/docs/research/disaster-fraud.pdf

On June 9, 2008, the U.S. District Court for the Southern District of Texas sentenced eight defendants for their roles in a FEMA fraud conspiracy involving more than 70 applications for Katrina and Rita benefits on behalf of residents in area apartment complexes who were not victims of the hurricanes. The leader of the group was sentenced to 33 months in prison and ordered to pay $92,958 in restitution.

→ www.justice.gov/archive/opa/pr/2008/October/08-crm-877.html

---

Following the Grenfell Tower fire in 2017 an individual falsely claimed over £95k of government support by fraudulently claiming he was sleeping in Grenfell at the time of the fire.

→ news.met.police.uk/news/man-jailed-for-fraud-in-relation-to-grenfell-tower-fire-388507

During the Australian Bush Fire crisis in 2019/20, several instances were identified where individuals and groups were setting up fake fundraising initiatives for personal gain.

→ www.9news.com.au/national/australia-bushfires-scam-watch/3fa5ad36-58ec-4395-be32-07e4def0e69a

---

Annex **B**

Annex B – Good Practice in Fraud Risk Assessment

The key to dealing with fraud in any situation is through having a fraud risk assessment. A fraud risk assessment details who might defraud a system, how they could do it. It also includes what the likelihood and impact of it coming to pass are. The key fraud risks from the fraud risk assessment should be understood by those responsible for leading the emergency management. The following provides good practice on fraud risk assessment.

Ideally fraud risk assessments should be completed by resources who are experienced in fraud control and management. They should understand fraud, be familiar with a broad variety of fraud types and have a good understanding of how to produce a fraud risk assessment. They should be capable of simplifying the fraud risk assessment and communicating it to key stakeholders.

Fraud risk assessment is a creative process. It involves looking at policies and processes and creatively exploring how someone could commit fraud against it. It is not a process where the business looks to find factors that rationalise why fraud may not happen in their policies or processes. The process of developing a fraud risk assessment, information can be gathered on past frauds against similar policies or processes. However, this information should not be overly depended on, as there are likely to be many more risks than those that can be identified through previously detected fraud.

Good fraud risk assessments have specific fraud risks, laid out in the 'Actor, Action, Outcome' formula. The more specific a fraud risk is, the more able the business will be to take effective action. For instance, a fraud risk of 'A member of the public will misdeclare their circumstances to gain support to which they are not entitled' is more difficult to identify effective counter-measures for than 'a member of the public will falsely declare they were living in x location at the time of the emergency to gain support to which they are not entitled'.

Documented fraud risks must be specific and if they happen will lead to fraud. It is not a cause or other factor. For instance, a fraud risk is 'A member of the public will claim that their property was flooded and damaged when it was not, to get access to financial support to which they are not entitled'. 'Uncertainty around processes' or 'lack of audit resources' are not fraud risks. They are factors or drivers that increase the likelihood or fraud coming to pass.

Once fraud risks are established, the fraud risk assessor identifies the counter-measures of controls in place that mitigate them. In doing this, it is important that the weaknesses and limitations of the controls are also established.

Giving consideration to the controls, the fraud risk assessment should establish the residual risk (the risk after the controls are applied). The residual risk should be described in full – stating how the fraud could still happen, rather than defining it as high/medium/low. From this description, the risk should be scored for the likelihood of occurrence, and the impact should it occur. This is usually done on a score of 1-5 for each factor (1 being low, 5 being high). From

these scores, this enables the risks to be prioritised, tolerances set, and consideration given to what risks should be reduced through additional counter-measures. Where new controls or counter-measures are introduced, the risks should be reassessed.

Annex **C**

Annex C – Examples of effective counter-measures to be considered

Once you have identified where you may be defrauded in an emergency management context, it is important to implement low friction controls where possible.

The controls that are put in place will be specific to the policies and processes that are being operated, as well as the risks that these lead to. For instance, if the emergency management situation is the provision of grants for communities to help rebuild after a natural disaster, the fraud risks will depend on what criteria is set for individuals or groups to be eligible for these grants, and what the grants are allowed to be spent on.

Due to the specific nature of fraud risk, and effective counter-measures, the counter-measures listed in this annex are higher level counter-measures that may reduce the overall level of fraud risk, rather than effectively mitigate the specific fraud risks that the emergency management situation faces.

The most effective way to manage fraud risk remains to understand the detailed risks and having corresponding counter-measures. In emergency management situations the inherent risk of fraud will remain high. However, when working at pace, these high level counter-measures will reduce some of the risks and help to tackle future fraud.

Use existing systems and criteria where possible

In emergency management situations, systems, processes and policies (including the criteria for services and payments to be made appropriately) are created at pace and can carry higher levels of uncertainty and change than standard policies and processes. Those leading the response can also struggle to resource the recording of criteria and processes.

An effective way to mitigate the enhanced risk of fraud that this brings can be to utilise existing systems and criteria (for payments and services where possible). For instance, services to rebuild damaged infrastructure could use existing processes for the build and repair of infrastructure. Alternatively, support of those experiencing hardship as a result of a crisis could be linked to eligibility criteria for other public services.

Work with well-established, tried and tested partners where possible

When engaging with partners to deliver emergency management, there can be limited time to carry out upfront due diligence or fit for purpose checks to the extent that would be expected in other circumstances. This can lead to a higher risk of fraud as the organisation may be working with partners of whom they have very limited assurance.

To a certain extent, this risk can be mitigated by using tried and tested partners who have already been through due diligence regimes. However, this does not remove the risk of fraud, as fraud is committed by individuals, not organisations, and there is still a risk that individuals in the organisation will be motivated to commit fraud, or people will join the organisation and commit fraud.

Make sure payments are processes by limited staff with appropriate oversight

Allowing a large number of staff to process requests increases the risk that someone may deliberately process fraudulent claims, or be coerced into doing so. Limiting access to processing payments to specialised users during disaster response can reduce this risk. In addition, it is prudent to make sure that payments are monitored by someone post event to checking of regularity of payments. This limits the opportunity for an internal staff member to abuse their position, makes staff aware that checks are in place and makes it easier to identify fraud if it happens.

Collect and retain records of payments and services delivered

Fraudsters can take advantage when staff: are not aware of fraud, cannot identify where fraud is happening, miss red flags that it may be happening and do not know what to do when they find fraud. When building policies and processes around emergency management, those managing the response should, wherever possible, retain: records of payments, services delivered, and the evidence provided to demonstrate that services were delivered or individuals were eligible for the services or payments. This will make post event assurance more efficient and effective and may act as a deterrence to those who would commit fraud.

Train staff to identify and report fraud

Staff awareness of fraud is a key control. A significant amount of fraud is detected through tip-offs. Fraudsters can take advantage when staff are not aware of fraud, cannot identify where fraud is happening, or red flags that it may be and do not know what to do when they find fraud. It means they are less likely to be detected, and it makes fraud more likely to become endemic. By training staff to be aware of fraud and how to report it and ensuring they receive regular messages on fraud awareness, you can improve the soft controls in the system and increase the likelihood that fraud is deterred and detected.

Clear counter-measures for the detection of fraud

In an emergency management environment, it is important that counter-measures are low friction, so they do not delay urgent payments or services. However, to support effective post-payment assurance activities, it is also important to collect and retain records of the payments made, services provided and documents used in applications or interactions. Without these, the post-event assurance will struggle to investigate further whether the original decisions were correct.

Collecting evidence can also act as a deterrent to fraudsters. For example, if the emergency support is for suppliers to provide advice to businesses in affected communities, and suppliers are required to produce evidence that the advice was given, this is likely to deter some fraudsters (those who would pretend to give advice where they have not) from committing fraud.