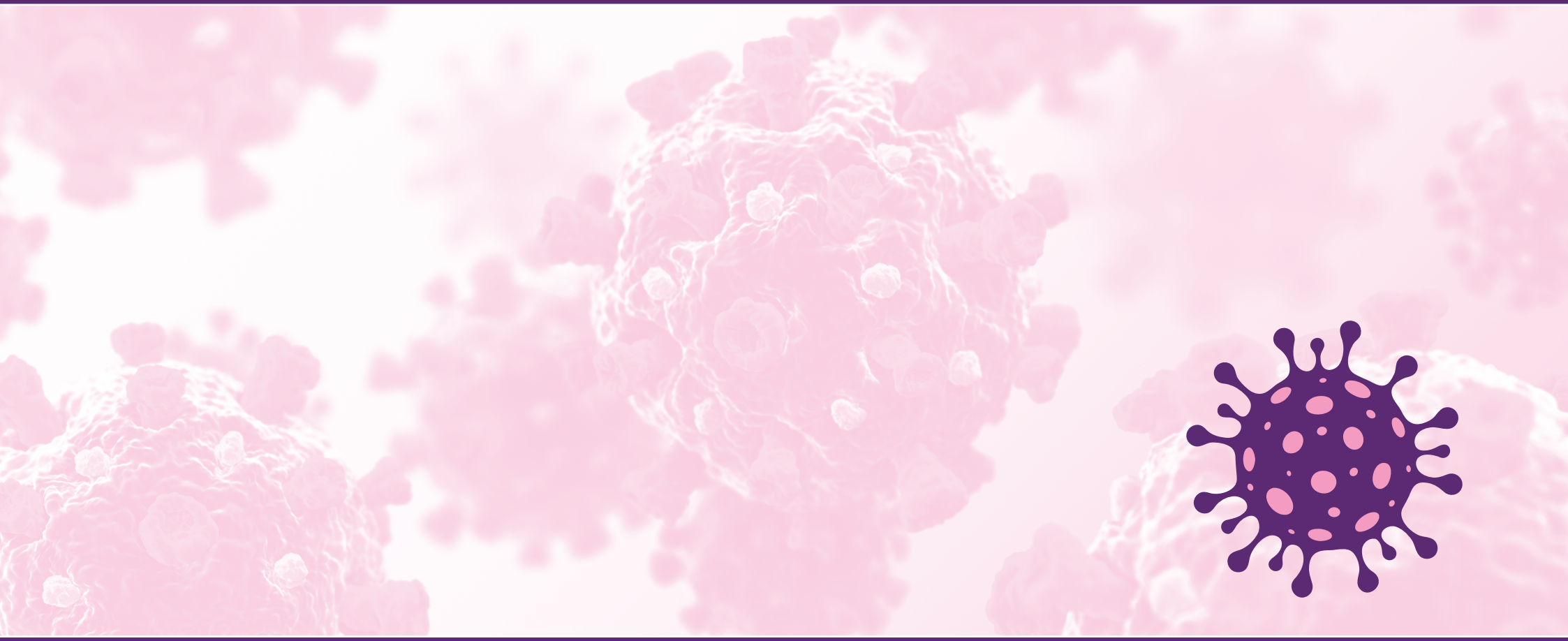
N I A O

Northern Ireland Audit Office

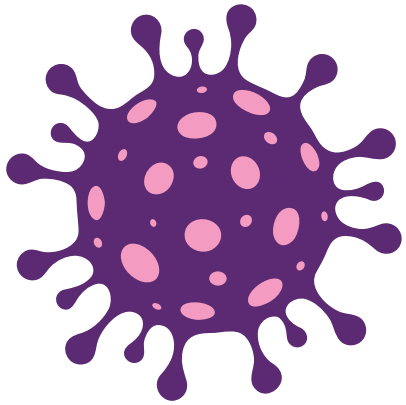
COVID-19 Fraud Risks



August 2020

Northern Ireland Audit Office

COVID-19 Fraud Risks



Northern Ireland Audit Office
106 University Street
BELFAST
BT7 1EU

Tel: 028 9025 1000
email: info@niauditoffice.gov.uk
website: **www.niauditoffice.gov.uk**

© Northern Ireland Audit Office 2020

COVID-19 Fraud Risks

It is widely accepted that fraud risks increase in times of change or crisis. The coronavirus pandemic and the resulting emergency measures put in place, for example the payment of business support grants, have significantly increased the opportunities for fraudsters. There is already clear evidence that fraudsters have been quick to seize upon such opportunities, with many stories in the media about organisations and individuals suffering financial loss as a result.

Raising awareness is key. Unless an organisation is alive to the new risks, it won't be in a position to mitigate those risks.

Many counter-fraud organisations have been pro-active in highlighting both existing and emerging fraud risks associated with the pandemic. This short Guide draws that information together to provide a quick point of reference for NI public sector organisations. It highlights the key risks and sets out the controls that can mitigate those risks.

Further information is available from a range of organisations, detailed at the end of this Guide.

Governance

Fraud Risks

Staff are working under extreme pressure in many organisations and, as a result, the application of internal controls is likely to suffer, with short-cuts taken.

Changes in staff deployment may result in staff shortages in some areas, with the application of internal controls compromised, or staff working in unfamiliar roles without a proper understanding of procedures and controls which should operate.

The operation of internal governance arrangements, such as a strong and active internal audit function and Audit Committee, may be disrupted during the crisis, leading to significant governance failures.

Normal channels for staff or third parties to raise concerns may be compromised due to staff re-deployment or furlough arrangements.

Mitigating Controls

- ✔ Undertake a fraud risk assessment. Identify new threats and risks and understand where normal controls may have been weakened. This will help to focus counter-fraud work as the pandemic continues. Internal audit will be a key function for this work.
- ✔ Continue to test internal controls, particularly in areas of increased risk.
- ✔ Ensure that staff reassigned to unfamiliar work are given an appropriate level of training or appropriate guidance and supervision.
- ✔ Be alert to unusual or suspicious freedom of information requests or other general enquiries. For example, could the information being requested be used by a fraudster to make a false claim for financial support?
- ✔ Maintain an active Audit Committee, even if it has to meet remotely, and ensure it is fully apprised of COVID-19 risks to the organisation and the measures being adopted to mitigate those risks.
- ✔ Ensure that there is still an effective route for employees, suppliers etc. to raise concerns about possible fraudulent activity.

COVID-19 Funding

Fraud Risks

As COVID-related grants are being administered at speed and online, there is an increased risk of grant applications being supported by fraudulent documentation.

The speed at which grant support schemes have to be administered will impact on the operation of normal controls, with due diligence procedures likely to be scaled back.

Fraudsters may try to acquire information from public sector organisations, through Freedom of Information requests or other general enquiries, which they can then use to support fraudulent grant claims.

Mitigating Controls

- ✔ Ensure that all COVID-19 grant forms include appropriate fraud prevention wording (i.e. that the data may be used/processed to detect potential fraud), to comply with fair processing requirements under data protection legislation. This will smooth the way for both upfront and post-event assurance checking, using data matching and data analytics.
- ✔ Collect consistent data in relation to grant applicants and grant recipients of COVID-19 financial support. Consistent, meaningful data, collected in line with data protection legislation, will facilitate effective post-assurance checking.
- ✔ COVID-19 financial assistance arrangements should include provision for clawback of funding, to enable recovery of funds paid out incorrectly.
- ✔ Where possible, implement upfront due diligence controls, such as checking the identity and status of the applicant before payment.
- ✔ Consider using available verification tools (such as Spotlight for grant verification, or the National Fraud Initiative's Appcheck for data matching).
- ✔ Consider accessing data held by other departments and agencies which could be used to validate or substantiate grant claimants' details.
- ✔ Devise procedures for ensuring that grant funding has been used appropriately, and invoke clawback arrangements where necessary.

Procurement

Fraud Risks

The pressure to secure additional supplies, particularly in the health sector, may lead to reduced due diligence in relation to new suppliers.

Reduced due diligence increases the opportunity for fraudsters to infiltrate the supply chain, particularly as online suppliers of scarce items. They may supply inferior or harmful items.

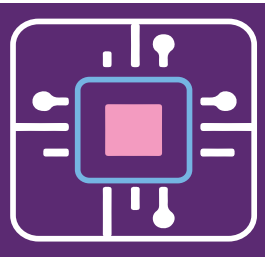
Added pressure on procurement staff may lead to more processing errors, for example duplicate payments or payments made for goods not received.

Fraudsters may exploit the fact that normal controls around procurement may be weakened and will seek to divert funds to their own accounts by purporting to be a supplier and notifying a change in bank account details.

Mitigating Controls

- ✔ Determine an appropriate balance between ensuring prompt supply and delivery and ensuring adequate due diligence in relation to new suppliers.
- ✔ Be aware of guidance on how to protect your supply chain, e.g. as provided by CIPFA.
- ✔ Maintain, as far as possible, normal internal controls around the supply chain, from ordering to payment.
- ✔ Remind staff of the increased risk of invoice/mandate fraud and make them aware of guidance to help minimise the risk, for example from the Fraud Advisory Panel.

IT/Cyber/Data Security



Fraud Risks

Large numbers of staff working remotely greatly increases the opportunities for breaches in IT protocols, e.g. staff linking personal devices to work devices.

Remote working may increase the risk of cyber-crime by allowing fraudsters to access organisations' systems through staff working from home. Staff may drop their guard when home working and, for example, click on links which they wouldn't normally do.

Fraudsters may use pandemic-related emails, purporting to be from government departments or agencies, to try and get staff to provide personal details which could be used for fraudulent purposes.

Security of personal data may be compromised due to remote working. An employee may leave confidential or sensitive information unsecured in their home environment or fail to lock computer screens when not in use, leaving the information visible and accessible to others in the household.

Remote working has led to a massive increase in the use of video conferencing and video calls, which can have susceptibilities.

Mitigating Controls

- ✔ Remind staff, through regular communications, that IT protocols around proper use of all devices must be observed at all times.
- ✔ Ensure staff are alert to the increased risk of fraudulent emails which, if responded to, could compromise system security.
- ✔ Remind staff that personal details should never be provided in response to unsolicited emails, even if they appear to be from legitimate sources.
- ✔ Remind staff that the standards of data security expected in the office environment should still be observed in the home-working environment, especially in relation to sensitive personal data.
- ✔ Ensure your organisation is aware of guidance on the safe and secure use of video conferencing platforms, for example from the National Cyber Security Centre.

Payroll/Recruitment

Fraud Risks

The financial impact of COVID-19 on a household's income (e.g. due to furlough or redundancy) may mean staff are tempted to make up any shortfall through, for example, false claims for overtime or expenses, aware that normal controls may not be fully operating.

The pressure to recruit additional staff in certain key areas, in a short timescale, may lead to increased recruitment fraud, e.g. use of fraudulent documentation to support applications. This is a particular risk in sensitive areas such as social care.

Mitigating Controls

- ✔ HR/payroll staff must be made aware of the increased risks and ensure that controls remain robust.
- ✔ Any changes to processes or systems due to COVID-19 arrangements should be explained to staff and compliance ensured.

Staff

Fraud Risks

The possible financial pressures on families as a result of the COVID-19 pandemic may lead to an increase in internal fraud (pressure/motivation is one side of the fraud triangle – see pages 4-5 of the document linked below).
https://www.niauditoffice.gov.uk/sites/niao/files/media-files/fraud_good_practice_guide.pdf

Remote working and internal controls operating at a sub-optimal level will increase the opportunity for internal fraud (opportunity is another side of the fraud triangle).

Staff working with vulnerable people, for example in the social care sector, may use COVID-19 as a cover for taking advantage of their clients, e.g. offering to do shopping but taking more money than is required.

Working under pressure, in isolation, and with inadequate support may increase the level of employee errors.

Mitigating Controls

- ✔ Organisations should be aware of the fraud triangle and how the current situation has increased pressure and opportunity for internal fraud. These factors should be taken into account in a fraud risk assessment (see Governance above).
- ✔ Organisations should ensure that staff working remotely have contact with team members, have access to suitable support arrangements and are given advice on how to adapt their working practices during home working to ensure continued effectiveness and wellbeing.

Sources of guidance

A number of organisations provide COVID-19 counter fraud advice and guidance on their websites, including:

- Government
  - https://www.gov.uk/government/publications/fraud-control-in-emergency-management-covid-19-uk-government-guide
  - https://www.gov.uk/government/publications/coronavirus-covid-19-fraud-and-cyber-crime
- NHS Counter Fraud Authority – https://cfa.nhs.uk/fraud-prevention/COVID-19-guidance
- Action Fraud – https://www.actionfraud.police.uk/campaign/covid-19-guidance-and-advice
- Fraud Advisory Panel – https://www.fraudadvisorypanel.org/covid-fraud-watch-group/
- National Cyber Security Centre – https://www.ncsc.gov.uk/
- Audit Scotland – https://www.audit-scotland.gov.uk/uploads/docs/report/2020/briefing_200723_covid.pdf
- International Public Sector Fraud Forum – https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/864310/Fraud_in_Emergency_Management_and_Recovery_10Feb.pdf

Published by CDS

CDS 242165