Fraud and irregularity 2021/22

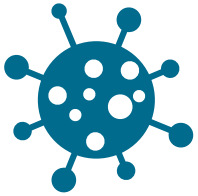
Sharing risks and case studies to support the Scottish public sector in the prevention of fraud

AUDIT SCOTLAND

Prepared by Audit Scotland for public bodies and auditors
July 2022

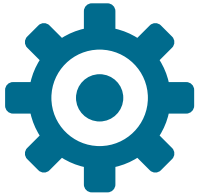
Key messages

The Covid-19 pandemic heightened the risk of fraud as new systems and ways of working were introduced.



1. The Covid-19 pandemic introduced many challenges for the Scottish public sector

Public Bodies delivered both existing and new services in new working environments. These changes resulted in additional fraud risks for public bodies to manage.



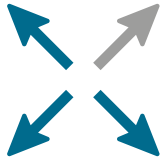
2. New challenges

Despite these new challenges, auditors have found that most bodies have responded well by introducing new systems, procedures, and controls.

Key messages continued

3. The Covid-19 pandemic has seen new fraud introduced

For example, fraudsters have targeted the grants to support businesses through the pandemic. Steps have subsequently been taken to reduce fraud and error in these schemes by grant-paying bodies and government.



4. Weaknesses in controls contributed to seven cases of fraud and irregularities totalling over £354,000

During 2021/22, internal control weaknesses contributed to seven cases of fraud and irregularity valued at over £354,000 being identified in public bodies. In comparison, 13 cases of fraud and irregularity valued at £401,500 were identified during 2020/21. Despite many challenges facing public bodies over the past two years because of the Covid-19 pandemic, the value of fraud and irregularity detected remains low compared to the 2021/22 annual Scottish budget of £54 billion.

Audit Scotland's counter-fraud hub contains useful counter-fraud information.

Recommendations

Public bodies should ensure effective counter-fraud arrangements are in place. These include:

- having effective governance and oversight arrangements for counter-fraud
- understanding the current and emerging counter-fraud risks facing the body
- regularly reviewing their counter-fraud strategy and counter-fraud plan
- regularly assessing and reviewing internal controls and governance arrangements to ensure they remain effective
- considering whether the risks and weaknesses in controls identified in this report may exist in their organisation and taking appropriate corrective actions
- reviewing the independent reviews and associated recommendations that were commissioned by the Scottish Environment Protection Agency (SEPA) following a ransomware attack on its systems.

Auditors should confirm that:

- the governance arrangements in place in their audit clients are effective, regularly reviewed and amended as appropriate for new fraud risks
- internal controls are operating effectively to help prevent fraud and irregularity, including the examples detailed in this report.

Fraud and irregularity identified during 2021/22

Auditors have provided Audit Scotland with details of cases of fraud and other irregularity discovered in their audited bodies during 2021/22. This report sets out examples of the various categories of fraud and irregularity reported during 2021/22 and the control weaknesses which contributed to these cases.

Aims of this report

This report shares information about cases where internal control weaknesses in public bodies have led to fraud and irregularity, to help prevent similar circumstances happening again. External auditors have shared specific details about significant frauds and other irregularities in public bodies during 2021/22. The level of fraud and irregularity reported by external auditors was over £354,000, which is a very small proportion of the 2021/22 Scottish budget of £54 billion.

External auditors are required to report frauds, or suspected frauds, to Audit Scotland where they are caused or facilitated by weaknesses in public bodies' **internal controls**. Frauds and irregularities are considered significant where the value of the loss is over £5,000 or where it is of significance owing to the nature of the activity.

The cases included in this report are likely to have been investigated internally, but it is not necessary for the police to have been involved or for it to have been proven as fraud in a court of law.

Reporting cases about fraud and irregularity and sharing information about what happened helps highlight weaknesses in internal controls and aims to help prevent similar circumstances from happening in other public bodies.

Internal controls help organisations to respond to risks, to comply with legislation and regulations and to prepare quality financial information. This includes policies and procedures organisations put in place to help prevent errors and irregularities.

Public bodies are encouraged to consider whether the weaknesses in internal control that facilitated each of the cases highlighted in this report may also exist in their own arrangements and take the required corrective action.

Fraud and irregularity identified during 2021/22

Fraud and irregularity reported during 2021/22 totals over £354,000 and falls into the following categories:

1 case
Pension fund

1 case
Procurement cards

1 case
Invalid supplier

1 case
Ticket income

2 cases
Covid-19 funding - 2 cases are included in this report as examples.

1 case
IT and cybercrime

Control weaknesses

The fraudulent and irregular activity reported by external auditors during 2021/22 highlighted control weaknesses which contributed to the fraudulent and irregular activity.

Not checking customer details are up to date

Procedures not followed

Weak IT security arrangements

A lack of staff training

A weak authorisation process for payments

Easily circumvented procedures

Specific details of the fraud and irregularity are reported on the following pages.

Pension fraud

Pension fraud relates to people receiving payments from a pension fund to which they are not entitled.

Case Study 1: Pension fraud

A family member of a deceased pensioner continued to collect £300,000 of pension payments over a 31-year period from a public sector pension fund.

Key features

The pension fund was not notified of the death of the pensioner and the pension payments continued to be paid.

The fraud was discovered by the pension fund after mail sent to the deceased pensioner was returned.

The fraud was possible as the pensioner's death pre-dated data-matching controls which are now in place to automatically highlight when a pensioner has died.

The pension payments have been stopped and the matter reported to Police Scotland.

Expenditure fraud

Expenditure frauds relate to cases where a body has incurred additional expenditure because of fraud. This may be due to invalid suppliers, fictitious invoicing, or the redirection of payments intended for legitimate suppliers.

Action Fraud UK is the national centre where individuals can report fraud and cybercrime.

Case Study 2: Corporate procurement card fraud

A council employee misused a corporate procurement card to fund personal purchases valued at over £7,300.

Key features

The employee used an emergency authorisation process to bypass the requirement to obtain authorisation at a local level. It was therefore not identified that the purchases were not legitimate. The employee also dishonestly accessed emails and misused a computer system to fraudulently authorise their own purchases.

The fraud was identified through budgetary control processes.

The employee has been dismissed and reported to the Procurator Fiscal. Two managers are also subject to the council's disciplinary procedures.

The council has since provided staff with detailed instructions and training which outline the proper process for using and authorising corporate procurement cards.

Case Study 3: Invalid supplier

A third party defrauded over £23,000 from a public body by purporting to be a supplier to the body.

Key features

The public body received a request by email to amend a supplier's bank account details. The supplier's email address had been intercepted by a fraudster who requested the change.

The fraud was possible as the public body did not telephone the supplier to verify the change of bank details.

The issue was identified when the genuine supplier queried why the payment had not been received.

The public body's internal audit team has reviewed the process for changing suppliers' bank account details. Improvements have been made to procedures and training has been provided for relevant staff.

The matter has been reported to Police Scotland and **Action Fraud UK** has also been notified of the case.

Income fraud

Income fraud relates to cases where a body has lost income because of fraud.

Case Study 4: Admission ticket income

Third parties defrauded over £8,600 in admission ticket income from a public body.

Key features

Unknown third parties fraudulently purchased and then resold admission tickets for events. The purchases were made using credit cards issued by an international provider. A loss was incurred as tickets had been used before the fraud was identified.

The fraud was discovered when the genuine cardholders subsequently requested refunds.

The fraud was facilitated by the international card provider not having secondary authentication procedures in place. The public body has stopped accepting credit cards without any secondary authorisation procedures in place.

Processes have been put in place to enhance card holder authentication for card payments.

Covid-19 funding fraud

Covid-19 funding fraud relates to cases where fraudulent funding applications have been paid.

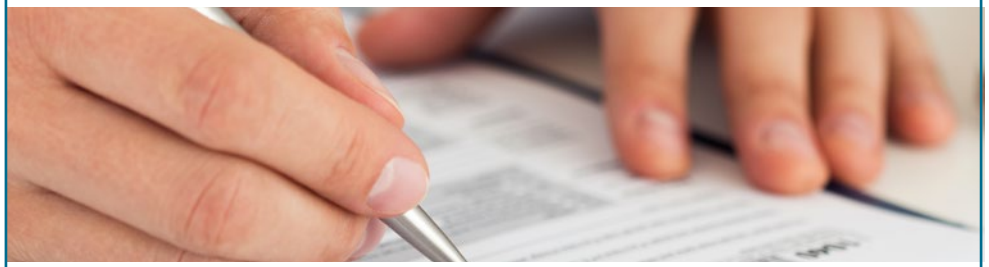
UK Government funding to the Scottish Government to support businesses and individuals throughout the Covid-19 pandemic was provided quickly, and often with lower levels of scrutiny and due diligence than are normally in place. Support was often provided to individuals and businesses that the paying organisation had no previous relationship with. This made verification of claims for funding difficult. To get the funding out quickly to those in need, the Scottish and UK governments introduced schemes which relied on self-declaration by the claimant.

This has resulted in applicants being paid funding which subsequently have been found to have been fraudulent.

The value of some **grants** paid by councils depended on the type of business and the rateable value of the business premises.

Case Study 5: Covid-19 funding (1)

A council paid out a £10,000 Covid-19 business support **grant** which later was discovered to be fraudulent.



Key features

A fraudster submitted an application supported by a forged lease document for the business premises and a forged bank statement. A previous fraudulent change in ratepayer had been notified to the council.

The fraud was identified when the legitimate applicant submitted a grant application.

A second subsequent application has since been made for another grant in a subsequent grant-funding phase. The council did not process this second application.

The council has shared the details of the fraudulent application with other public bodies and has notified Police Scotland.

Covid-19 funding fraud (continued)

Case Study 6: Covid-19 funding (2)

A public body paid out a grant of £5,250 to a business based on an application having been received with a self-declaration by the business. The business stated that it had been adversely impacted by Covid-19. The public body paid out funds in accordance with the instructions and procedures issued by the Scottish Government.

Key features

The public body subsequently received a communication from a third party highlighting concern over the award of the funding to this business. The public body's internal audit team carried out a review and requested further supporting evidence. This established that the recipient did not meet the eligibility criteria for the funding.

The public body is seeking recovery of the grant paid.

Cybercrime

Cybercrime relates to losses due to crime which has been committed using computer systems and IT networks.

Case Study 7: Cyber-attack

SEPA suffered a cyber-attack and subsequent data loss on 24 December 2020. Our 2020/21 Fraud and irregularity report contained initial details which were known at that time. Further details and learning from the attack are now available and a summary is provided below.

Key features

The cyber-attack resulted in SEPA being unable to retrieve a significant amount of its data. This was despite independent reviews finding that SEPA had a high level of cyber security maturity. The criminals demanded a ransom which SEPA did not pay.

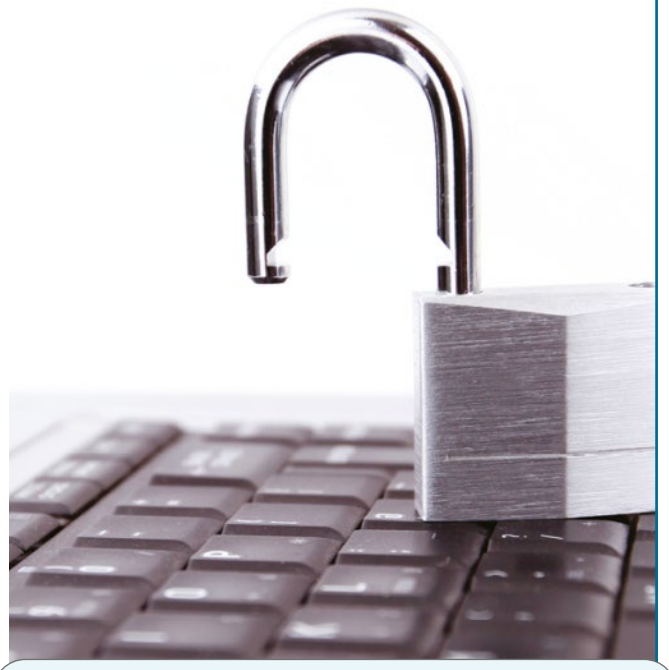
Investigations have not yet identified the exact route source of where the cyber-attack breached SEPA's systems. However, there are indications that it was through a **phishing** attack. This means there may have been a degree of human error involved, which is very difficult to mitigate against.

SEPA immediately implemented its emergency management arrangements in response to the cyber-attack. It also worked with the Scottish Government, Police Scotland, the National Cyber Security Centre (NCSC) and the Scottish Business Resilience Centre (SBRC) to deliver a recovery strategy.

SEPA commissioned independent reviews to assist it and other public-sector organisations in learning from the incident and to help protect itself and others from ongoing cyber threats. The independent reviews identified a number of recommendations.

Public-sector bodies should review these recommendations and learn lessons from what has happened to SEPA. This incident highlights that no organisation can fully mitigate the risk of the ever-increasing threat and sophistication of a cyber-attack but it is crucial that organisations are prepared.

The Auditor General has published a report on the cyber-attack against SEPA.



Phishing is where criminals send emails purporting to be from reputable sources to deceive individuals into providing information or data such as passwords, or to click on a link that allows malware to be downloaded.

Ways to reduce counter-fraud risks

There are many ways that public bodies can attempt to mitigate the risk of fraud as well as trying to prevent fraudulent activity from occurring. This includes:

- understanding the organisation's fraud risks. An appropriate counter-fraud strategy and plan should be in place
- ensuring appropriate governance arrangements are in place, with oversight of counter-fraud arrangements
- agreeing the organisation's fraud risk appetite and approach to newly-emerging risks
- having appropriate fraud prevention and detection processes in place
- regularly carrying out a fraud risk assessment to identify vulnerable areas
- having internal audit regularly reviewing and evaluating controls to ensure they operate effectively and can adapt to new or emerging risks
- ensuring staff are appropriately trained in their area of work. This will include counter-fraud training specific to their role
- ensuring processes are in place to report any suspected fraud or error
- having effective fraud response arrangements in place
- reviewing any instances of fraud or error for any lessons that could be learnt to prevent future losses
- using digital innovations, eg data analytics, to help identify weakness in controls
- using data matching such as the National Fraud Initiative **(NFI)** and analytical procedures to help identify fraud or error
- working collaboratively with partners to prevent and detect fraud
- ensuring IT systems are protected and the latest guidance from bodies such as the National Cyber Security Centre is followed.

The NFI is a data matching exercise that matches electronic data within and between public and private-sector bodies to prevent and detect fraud.

Further information

Further information about Audit Scotland's work to support counter-fraud and good governance is available on our website. This includes information about:

Website:
Our work on counter-fraud

Report:
Covid-19: Emerging fraud risks
July 2020

Report:
Red flags in procurement
October 2019

Website:
The National Fraud Initiative

Blog:
Cybercrime: A serious risk to Scotland's public sector
May 2021

Report:
How councils can safeguard public money
April 2019

Report: **The 2020/21 audit of the Scottish Environment Protection Agency**
February 2022

Fraud and irregularity
2021/22

Audit Scotland's published material is available for download on the website in a number of formats. For information on our accessibility principles, please visit:
www.audit-scotland.gov.uk/accessibility

For the latest news follow us on social media or **subscribe to our email alerts**.

AUDIT SCOTLAND

Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN
Phone: 0131 625 1500 Email: **info@audit-scotland.gov.uk**
www.audit-scotland.gov.uk

ISBN 978 1 913287 90 0