

**REPORT TO: SCRUTINY COMMITTEE – 22 SEPTEMBER 2021**

**REPORT ON: CORPORATE FRAUD TEAM ACTIVITY & PERFORMANCE,  
INCLUDING WHISTLEBLOWING 2020/21**

**REPORT BY: EXECUTIVE DIRECTOR OF CORPORATE SERVICES**

**REPORT NO: 259-2021**

## **1.0 PURPOSE OF REPORT**

This report is to inform Elected Members of the Corporate Fraud Team's (CFT's) activity and performance for the 12-month period to 31 March 2021, including whistleblowing activity, as well as provide a summary of key messages from Audit Scotland's Fraud and Irregularity 2020/21 national report surrounding emerging fraud risks since the start of Covid-19.

## **2.0 RECOMMENDATIONS**

It is recommended that Members of the Committee:

- i. note the content of the CFT's activity and performance report for 2020/21 at Appendix 1, including referral statistics and savings / other benefits identified during the year;
- ii. note the results of the Council's whistleblowing activity for 2020/21 at Appendix 2, including allegation statistics and outcomes; and
- iii. Note the key messages from Audit Scotland's Fraud and Irregularity 2020/21 national report at Appendix 3.

## **3.0 FINANCIAL IMPLICATIONS**

In the year to 31 March 2021, the CFT identified savings of £405,630 from general investigative work and £187,238 of fraud and / or error in Housing Benefits through the sharing of intelligence with the Department of Work and Pensions (DWP) Single Fraud Investigation Service (SFIS). With the exception of notional savings and prevented payments, action has been taken by the Council to seek financial recovery.

## **4.0 BACKGROUND**

At the 27 April 2015 Policy and Resources Committee (Article VIII, Report No 180-2015) Members approved the establishment of a CFT from 1 June 2015. The CFT is a specialist investigative unit with responsibility for investigating all types of corporate fraud.

### **4.1 COVID-19 PANDEMIC**

The restrictions brought about by Covid-19 impacted significantly on counter fraud work, most notably the requirement to stay at home, cease face to face investigatory meetings, visits and blue badge misuse investigations. In addition, DWP SFIS investigations stopped for a period of time and, consequently, the sharing of information via the Local Authority Information Exchange Forms paused simultaneously.

As a result of the above, for the period April 2020 to July 2020, all 4 members of staff from the CFT were redeployed in some capacity to help the organisation's Covid-19 response efforts, at the same time as dealing with CFT related demands. The range of assistance provided was diverse and included:

- the establishment, and day to day operational delivery, of the Michelin distribution centre for PPE and emergency food boxes;
- making telephone calls to clients regarding free school meal entitlement;
- data matching assistance surrounding self-employed hardship applications; and
- the provision of ad-hoc shopping and delivery services for some of Dundee's most vulnerable residents.

Throughout 2020/21, the CFT worked alongside services and Internal Audit and Risk colleagues to help the Council mitigate the risk of fraud that had emerged as a result of the Covid-19 pandemic. More specifically, the CFT worked with key members of staff in the teams responsible for administering the various Business Support Grants. At the same time, to help raise staff awareness surrounding fraud risk relating to Covid-19 grant applications, the CFT delivered targeted training.

The CFT investigated 164 suspected fraudulent / incorrect applications relating to the Covid-19 Strategic Framework Business Fund (SFBF). These investigations prevented £381,500 payments being incorrectly awarded via 143 applications. In the same period, for context, the Council administered Covid-19 related grants totalling of the order of £47m.

The CFT also worked in collaboration with other Scottish local authorities to maintain a list of suspected fraud cases. The accumulated list was shared with relevant Council officers to help facilitate appropriate cross-checking of information prior to payment and ultimately mitigate the risk of paying fraudulent claims.

During the financial year, the Cabinet Office, Police Scotland and Audit Scotland all issued publications on Covid-19 emerging fraud risks for the public sector and these have all been fully considered and, where appropriate, utilised by the CFT. Covid-19 Fraud Intelligence alerts received from third parties, including other local authorities, the Scottish Local Authority Investigator's Group (SLAIG), the National Anti-Fraud Network (NAFN) and Police Scotland were also shared timeously with key officers.

## **4.2 GENERAL INVESTIGATIVE WORK AND SFIS**

The CFT identified £405,630 of savings in the year to 31 March 2021, which includes the prevention of £381,500 Covid-19 SFBF payments (as noted above at 4.1), as well as notional savings of £4,000 relating to blue badge cases and £18,000 from a Tenancy Fraud case. With reference to Article XVI, Report No 84-2015 of the Policy and Resources Committee held in February 2015, the notional value allocated to the termination of each blue badge is £2,000 and the notional value allocated to each tenancy returned to the Council is £18,000.

When SFIS activity re-started surrounding Housing Benefit investigations, the CFT assisted through the sharing of intelligence; during the year to 31 March 2021, that work identified £187,238 of fraud and error. Further detail is included at Appendix 1 along with referral statistics for the year.

The CFT continues to work with and share best practice with various other agencies and public sector bodies. These include various teams within Police Scotland, Scottish Government, Audit Scotland, OSCR (Office of the Scottish Charity Regulator), the Cabinet Office, SEPA (Scottish Environment Protection Agency), NHS Fraud Services, SAAS (Student Award Agency Scotland), HMRC and other Scottish local authorities.

### **4.3 ADVICE, GUIDANCE AND CORPORATE SUPPORT**

In addition to the investigative work carried out during 2020/21, the CFT has continued to provide a diverse range of advice, guidance and support to the Council's strategic services, DH&SCP and Leisure & Culture Dundee (L&CD).

The CFT continues to assist the Council's Parking Team and the Sheriff Officers to trace debtors with large outstanding debts relating to non-payment of Penalty Charge Notices. The new information obtained by the CFT is shared with the Sheriff Officers to assist in the debt recovery process. As in previous years, the CFT will continue to provide investigative support for the recovery of parking debt.

Work carried out by the CFT during 2020/21 continued, once again, to evolve in the Council. In addition, the CFT has continued to be actively involved in operational groups and processes, including the Serious Organised Crime Group, Integrity Group and the Compliance Group (see 4.5 below), all of which are chaired by the Head of Corporate Finance.

The Council's Integrity Group, which meets regularly, receives, considers and monitors organisational vulnerability alerts / fraud and corruption flags identified via a number of sources, including intelligence from external bodies, and agrees appropriate actions / preventative measures to mitigate the risks identified. At the Scrutiny Committee Meeting on 17 April 2019, Elected Members received the Council's first Corporate Integrity Group Report (Article VIII, Report No. 155-2019). In 2020/21, 2 Whistleblowing allegations were brought to the attention of the Integrity Group. These investigations were fully investigated by the CFT and HR. The first allegation was unproven. The second resulted in a member of staff resigning after being interviewed by the CFT and subsequently being notified that disciplinary procedures would commence. Members of the Integrity Group were regularly updated during both investigations.

The CFT Supervisor's work in the Council's Serious Organised Crime Group included the compilation and publication of a Guide to Serious Organised Crime (SOC) for staff on OneDundee and, in conjunction with the Corporate Risk Management Co-ordinator, development of a draft collaborative SOC Risk Register.

The CFT Supervisor has continued during 2020/21 to be the Scottish representative on the Executive Board of NAFN and an active member of SLAIG, both of which have continued to meet remotely. As part of SLAIG, the CFT Supervisor participates in discussions with the Crown Office and Procurator Fiscal Service (COPFS) and Scottish Government regarding the ongoing prevention and detection of public sector fraud. The CFT also receives national fraud alerts through NAFN from the National Crime Agency, the National Fraud Intelligence Bureau and the National Cyber Security Centre. These alerts, which have included Covid-19 National Fraud Alerts this year, are distributed to key Council staff.

The CFT continues to work closely with the DWP and is represented at both local and national (Scottish) level meetings to help support the Housing Benefit investigation process in general and recovery of overpayments from Housing Benefit fraud and error in Dundee.

#### **4.4 COMPLIANCE GROUP AND RELATED CFT WORK**

A Compliance Group was established in 2019/20 within Corporate Finance to help ensure that a sound, consistent system of internal control exists across the Council. Membership of the core Compliance Group, which is chaired by the Head of Corporate Finance, is the Council's Senior Manager – Internal Audit, Senior Manager - Financial Services, Corporate Procurement Manager and a Senior Accountant. The work of the core Compliance Group, including prioritised engagement with Council services, is informed through a risk-based approach.

During 2020/21, the Compliance Group advised the CFT to carry out a review of all petty cash and cash advance requests received over a 6-month period. No concerns were identified during the course of the review work.

The Compliance Group also developed a control self-assessment checklist with corresponding best practice guidance documents, which were subsequently issued by the Head of Corporate Finance to all services for completion. The returned forms have been risk assessed by the CFT as well as other teams within Corporate Finance and guidance, control support and training will be provided in due course where areas requiring improvement are identified. Going forward, when it is safe to do so, the CFT will carry out ad-hoc establishment visits to review controls in operation and feedback assurances, or otherwise, to the Compliance Group.

In February 2021, general Government Procurement Card (GPC) and GPC fraud awareness training was delivered to GPC holders at secondary schools. The training was delivered by the Corporate Procurement Manager and CFT Supervisor via MS Teams. The training was designed to remind GPC holders of their personal responsibilities and increase awareness surrounding GPC fraud and risk.

#### **4.5 CORPORATE FRAUD EMPLOYEE INVESTIGATIONS**

Fraud and corruption are ever present risks in all organisations and can have a negative impact through disruption to services or undermining the achievement of objectives.

The Council acknowledges its responsibility for ensuring that fraud and corruption risks are mitigated and managed effectively. All allegations of fraud and corruption are investigated by CFT staff, in partnership with other Council colleagues and external agencies where appropriate.

During 2020/21, the CFT continued to investigate allegations of fraud, bribery and corruption, which at times involved working alongside Police Scotland and the COPFS. Through the investigations relating to those allegations, the CFT identified a number of risks. Recommendations were subsequently made to service areas to help improve internal controls, mitigate the risks and, in turn, strengthen the Council's governance arrangements.

Other CFT investigations during 2020/21 involving employees included allegations of improper conduct with contractors, missing cash and goods (including PPE), misuse of Council / hire vehicles, GPC misuse, Council Tax Reduction and discounts, Blue Badge misuse, misuse of flexitime and annual leave system, breach of Scottish Government Covid-19 lockdown / level restrictions and breach of Council policies. Following conclusion of these investigations, recommendations for improvements to internal controls, to reduce the risk of similar incidents happening in the future, are passed to HR and the employee's Head of Service. It is the remit of HR and the employee's Head of Service to consider whether any disciplinary action is required.

#### **4.6 WHISTLEBLOWING**

The Council's whistleblowing function is corporately managed by the CFT. In line with the policy, all whistleblowing allegations received are shared with the Head of Human Resources and Business Support, the Head of Democratic and Legal Services and the Senior Manager – Internal Audit. These managers, or an appropriate delegated officer, determine how best to proceed with, and who should lead, an investigation.

The action taken by the Council in response to a reported concern will depend on its nature, but may include one or more of the following:

- carrying out an internal investigation (HR, Internal Audit and / or CFT)
- dealing with the matter through an internal procedure
- referring the issue to Police Scotland and / or to external audit
- referring the issue to an external public or regulatory authority
- bringing in external specialists to investigate where required

A decision may also be taken that no formal investigation is required.

Employees can report concerns in a variety of ways e.g. speak to their supervisor, send a letter, complete an anonymous form on the intranet or internet, email the dedicated email address or phone the 24hr freephone whistleblowing telephone number.

The CFT manages the Council's dedicated whistleblowing telephone line and email reporting arrangements. It also monitors and records all whistleblowing allegations and outcomes on the Council's Fraud Management System. For the 12-month period to 31 March 2021 the Council received 26 whistleblowing allegations, including one for L&CD, which is in line with last year's figure. The number of allegations received demonstrates the ongoing positive culture of the organisation in which staff feel comfortable enough to report their concerns. Whistleblowing allegation statistics, split by service area, can be found at Appendix 2 along with corresponding outcomes data.

#### **4.7 NATIONAL FRAUD INITIATIVE (NFI)**

The NFI is co-ordinated by the CFT and the Council's Key Contact is the CFT Supervisor. The Council's NFI performance is reported in a separate annual report to this Committee.

#### **4.8 AUDIT SCOTLAND'S FRAUD AND IRREGULARITY 2020/21 NATIONAL REPORT**

In July 2021, Audit Scotland published a report entitled Fraud and Irregularity 2020/21, a full copy of which can be found at Appendix 3.

As the Covid-19 pandemic continues to bring significant challenges across the Scottish public sector, the risk of fraud and error has increased. The report provides suggestions to public bodies on what they may do to help them identify, manage and reduce risks. The following paragraphs provide a summary of the report and what the Council has been proactively doing throughout the year to mitigate risks.

Key messages communicated in the report are:

- Significant challenges due to Covid-19

- Wide range of action required to mitigate new risks
- Weaknesses in controls contribute to fraud and irregular activities

Fraud-related risks identified by external auditors over the last year have been grouped together into the following seven categories. They include, but are not limited to, risks associated with:

- Covid-19 funding and reopening of premises and services
- Health and wellbeing
- IT and cybercrime
- Governance
- Procurement
- Payment
- Payroll and recruitment

The Council's Covid-19 Recovery Risk Register, which was approved by the Policy and Resources Committee at its meeting on 24 August 2020 (Report No. 193-2020), identifies twenty key risks that cover all of the above themes. In addition, the Risk Management Annual Report, which was approved by Policy and Resources Committee on 25 January 2021 (Report No. 47-2021), provides a comparative review of the Council's Corporate Risk Register (CRR), associated service level risk registers (SRR's) and the Covid-19 Recovery Risk Register (C19 RRR). Fraud & Corruption is a risk that is contained within all SRR's and the C19 RRR identifies Fraud & Corruption as 'High' risk. One report recommendation was that Fraud & Corruption should be added to the CRR as a specific risk with an assessment of 'High'. This recommendation has since been implemented.

Throughout the pandemic, monthly reports from Pentana were issued to Executive Directors and Heads of Service, outlining overdue risk reviews and requesting that they be updated timeously.

The report recommends that public bodies should ensure good governance and counter-fraud arrangements are in place, including:

- having in place appropriate governance and oversight arrangements for counter-fraud
- regularly reviewing controls and governance arrangements to ensure they remain fit for purpose
- being alert to emerging fraud risks and where appropriate working with other to help alleviate these risks
- considering whether appropriate controls are in place to prevent to risks notified in this report materialising in their own organisation
- considering whether the weaknesses in internal control that facilitated each case of fraud or irregularity identified in the report may also exist in their own organisations, and taking the required corrective action

The report required external audit teams to confirm that:

- appropriate governance arrangements for the prevention and detection of fraud are in place at their audit clients and that appropriate reviews and amendments of controls have taken place in response to new ways of working
- internal controls at their audit clients are sufficiently strong to prevent the types of fraud and irregularity highlighted in this report.

During 2020/21, the Council's Internal Audit Service provided ongoing advice and guidance surrounding the development of new or changed systems and processes established to respond to the continuously evolving Covid-19 environment, including the Covid-19 business support grants. In addition, it also carried out a specific review to ensure that key business operations and their associated governance and control frameworks were appropriately and timeously established / re-established. The review also focussed on the key changes made to the recruitment and selection processes as a result of the COVID-19 pandemic.

The Council continues to highlight wider fraud risks to staff and the public through the publication of a regular Covid-19 Frauds and Scams bulletin.

## **5.0 POLICY IMPLICATIONS**

This report has been subject to an assessment of any impacts on Equality and Diversity, Fairness and Poverty, Environment and Corporate Risk. There are no major issues.

## **6.0 CONSULTATIONS**

The Council Management Team was consulted in the preparation of this report.

## **7.0 BACKGROUND PAPERS**

None.

**ROBERT EMMOTT**  
**EXECUTIVE DIRECTOR OF CORPORATE SERVICES**

**29 AUGUST 2021**

*This page is intentionally left blank*



**CORPORATE FRAUD ACTIVITY AND PERFORMANCE REPORT - 1 APRIL 2020 TO 31  
MARCH 2021**

**Table 1 – CFT Referrals / Information Exchanges Statistics**

<b>SERVICE AREA / FRAUD or ERROR TYPE</b>	<b>NUMBER OF REFERRALS</b>
Blue Badge	21
Council Tax (Council Tax Reduction and discounts)	28
Housing Tenancy	7
Children & Families	16
City Development	2
Construction Services	3
Corporate Services	4
Neighbourhood Services	10
L&CD	1
DH&SCP	1
Covid-19 Grant Application Forms	164
<b>SUB-TOTAL</b>	<b>257</b>
Housing Benefit - DWP Information Exchange for Investigation Cases	33
<b>TOTAL</b>	<b>290</b>

Table 2 – Savings / Benefits Identified

FRAUD_or ERROR TYPE	NUMBER CASES	OF	SAVINGS IDENTIFIED (£) / BENEFITS
Blue Badge (Notional)	2		4,000 (2 badges removed from 3 <sup>rd</sup> parties due to misuse)
Council Tax (Council Tax Reduction and Single Person Discount)	12		2,031
Covid-19 Grants (Prevention)	143		381,500
Housing Benefit (Identified during other CFT investigations)	1		99
Housing Tenancy (Notional)	1		18,000
<b>SUB-TOTAL</b>	<b>159</b>		<b>405,630</b>
Housing Benefit - DWP Information Exchange for Investigation Cases	10		187,238
<b>TOTAL</b>	<b>169</b>		<b>592,868</b>

The tables below provide a summary of results from the whistleblowing activity for 12 months to 31 March 2021.

**Table 1 – Whistleblowing Allegations per Service Area**

Service Area	No. of Allegations
Children & Families	6
City Development	1
Construction Services	7*
Corporate Services	1
Neighbourhood Services	7*
DH&SCP	3
L&CD (passed to L&CD to investigate, with recommendations from CFT, Legal, HR & Internal Audit)	1
<b>TOTAL</b>	<b>26</b>

\* Some contained the same information provided in a previous allegation.

In addition to the above, the Whistleblowing Reporting System received 6 allegations about local businesses breaching local Covid-19 rules. These allegations were passed to and investigated by the Council's Trading Standards Team.

**Table 2 – Outcomes of Whistleblowing Allegations**

Outcomes	
Ongoing	1 allegation
No further action / unsubstantiated	21 allegations
Dealt with in line with current HR procedures **	1 individual

\*\* 3 allegations received for this individual

# Fraud and irregularity 2020/21

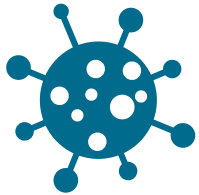
Sharing risks and case studies to support the Scottish public sector in the prevention of fraud



 AUDIT SCOTLAND

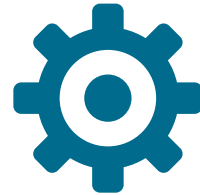
Prepared by Audit Scotland for public bodies and auditors  
July 2021

# Key messages



## 1. Significant challenges due to Covid-19

Since the start of 2020/21, the Covid-19 pandemic and the associated lockdowns have brought significant challenges across the public sector. Public bodies have sought to continue to deliver services in new working environments while at the same time experiencing an increase in demand for many services. The challenges during the last year include additional fraud risks for public bodies to identify and manage.



## 2. Wide range of action required to mitigate new risks

The new fraud risks cover a variety of areas. This means a wide range of actions are required by public bodies to attempt to mitigate these risks.



## 3. Weaknesses in controls contribute to fraud and irregular activities

Weaknesses in controls have contributed to a variety of fraud and irregular activities being identified across the Scottish public sector. During 2020/21, external auditors reported 13 cases of fraud and irregularity valued at £0.4 million. The value of reported fraud and irregularity remains small compared to the 2020/21 annual Scottish budget of £49 billion.



## 4. Counter-fraud hub

Audit Scotland's [counter-fraud hub](#) contains useful counter-fraud information.

# Recommendations

## **Public bodies should ensure good governance and counter-fraud arrangements are in place, including:**

- having in place appropriate governance and oversight arrangements for counter-fraud
- regularly reviewing controls and governance arrangements to ensure they remain fit for purpose
- being alert to emerging fraud risks and where appropriate working with others to help alleviate these risks
- considering whether appropriate controls are in place to prevent the risks identified in this report materialising in their own organisation
- considering whether the weaknesses in internal control that facilitated each case of fraud or irregularity identified in this report may also exist in their own organisations, and taking the required corrective action.

## **Auditors should confirm that:**

- appropriate governance arrangements for the prevention and detection of fraud are in place at their audit clients and that appropriate reviews and amendments of controls have taken place in response to new ways of working
- internal controls at their audit clients are sufficiently strong to prevent the types of fraud and irregularity highlighted in this report.

# Background

## Impact of Covid-19

The risk of fraud and error has increased over the last year due to the Covid-19 pandemic. This is due to many reasons, including:

- public bodies have become stretched, controls and governance arrangements have required to be changed
- staff working remotely and under pressure
- staff adapting to new ways of working with associated new processes and procedures
- staff being redeployed to work in new and unfamiliar departments as public bodies have responded to increased demands for certain services
- continuous fraud attempts on public bodies including both traditional types of fraud and newer cybercrimes
- former verification and control processes being unable to operate as new ways of working are introduced
- new support schemes for business and communities being developed and implemented at speed.

Public bodies need to review their systems and identify areas where the threat from fraud and error has increased. They need to review existing controls to ensure they are still effective and appropriate and at the same time introduce new controls to address new risks. Measures like these have always been important but the unprecedented challenges and pressures brought by the pandemic, and the opportunities it has presented for fraudsters, bring a renewed focus on ensuring effective governance and controls are in place.

Additional risks will continue to emerge as public money and services are targeted by fraudsters. Fraudsters will continue to look for new opportunities to exploit weaknesses in systems and controls. Public bodies and auditors should stay alert to new scams and approaches by fraudsters, and regularly review controls and governance arrangements to ensure they remain fit for purpose.

Good governance and sound controls are essential in crisis and changing situations.

## Aims of this report

This report sets out a range of fraud risks emerging since the start of the Covid-19 pandemic along with suggestions of what public bodies may do to help reduce these risks. It aims to help public bodies identify and manage these risks.

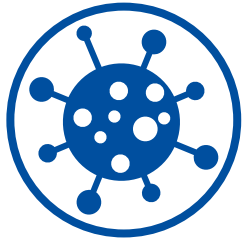
This report also shares information about cases where internal control weaknesses in public bodies have led to fraud and irregularity, to help prevent similar circumstances happening again. External auditors have shared specific details about significant frauds and other irregularities in public bodies during 2020/21. The level of fraud and irregularity reported by external auditors of £0.4 million remains small compared to the 2020/21 Scottish budget of £49 billion.

This report is informed by information provided by external auditors during 2020/21 in their fraud and irregularity returns to Audit Scotland. External auditors are required to report frauds (or suspected frauds) where they are caused or facilitated by weaknesses in internal controls at public bodies. Frauds and irregularities are considered significant where the value of the loss is over £5,000 or where it is of significance due to the nature of the activity.

Auditors of local authorities are not required to report cases of fraud perpetrated by claimants, for example, grant claimants or housing benefit claimants, unless the fraud was facilitated by the collusion of local authority staff or otherwise by weaknesses in internal control. 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.

# Key fraud risks identified in 2020/21

We have grouped the fraud-related risks identified by external auditors over the last year into the following seven categories. They include, but are not limited to, risks associated with:



**1. Covid-19 funding and reopening of premises and services**



**2. Health and wellbeing**



**3. IT and cybercrime**



**4. Governance**



**5. Procurement**



**6. Payment**



**7. Payroll and recruitment**





# 1. Covid-19 funding and reopening of premises and services

- Government stimulus packages to support individuals and businesses are provided quickly, possibly with a lower level of scrutiny and due diligence than has previously been in place. Often the support is provided to people and businesses that the public body had no previous relationship with, making the verification of details more difficult.
- Councils may receive emails or Freedom of Information requests asking for details about property details, reference numbers or business grant applications. Fraudsters are possibly looking to identify eligible businesses that have not applied for grants, with a view to submitting a fraudulent application.
- Councils may receive requests for business rate liabilities to be changed. This may be an attempt to ensure a business falls within a category qualifying for grants.
- Due to applications for Covid-19 related support being made online, there is a risk that fraudulent documents and details are provided.
- Councils may receive fraudulent applications for funding purporting to be from genuine qualifying businesses. These applications are often supported by what appears to be genuine supporting information which has often been obtained from publicly available sources.
- As buildings and offices reopen, emails may be received purporting, for example, to be from the Health and Safety Executive (HSE) saying the HSE is carrying out Covid-19 spot checks on newly opened premises. A link supposedly to guidance documents leads to a file which contains malicious software (malware).
- Texts may be received advising recipients that they are eligible for a Covid-19 grant and that an attached form requires to be completed. The form contains a link to a scam website, possibly similar to the HMRC website, asking for business, personal and bank details.

Additional Covid-19 related risks:

## **Covid-19: Emerging fraud risks**

July 2020





## 2. Health and wellbeing

- Remote working may result in isolation and/or mental health issues. This may lead, in some cases, to increased addictive behaviours (eg, gambling), which could result in vulnerability to serious organised crime gangs.
- An increase in internal fraud in public bodies is possible as staff and their families are under increased levels of financial and health pressures.
- Working for sustained periods of time at high levels of demand may lead to errors or fraud due to lapses in concentration.
- Staff/volunteers could take advantage of vulnerable service users, for example by gaining access to bank cards, cash drop-offs at client's house and befriending with sinister intentions.
- Emails may be received purporting to be from the NHS offering a Covid-19 vaccination. Recipients are requested to provide bank details.



## 3. IT and cybercrime

- Staff working remotely may pose potential security risks, eg when using personal devices and/or using removable devices to download data.
- Household members may gain unauthorised access to confidential information such as payroll, social work client details etc, by looking at screens or documents used by staff.
- Staff may be more likely to be tempted to steal data when working remotely without the normal office supervision.
- Staff working remotely may receive calls from fraudsters claiming to be legitimate technical support services and attempting to gain access to systems. The callers may say that they are looking at issues with the public body's network and will request the staff member's login details in order to 'fix' the system issue.
- Staff working at home may receive calls purportedly from their broadband providers. The caller says that they are having technical problems with the service. The caller asks the recipient to switch on their computer to check the broadband signal strength and then to enter a scam web address and/or download a piece of malware.
- There is a risk of increased cybercrime as more public-sector staff connect remotely to access systems and for meetings using online video conference services.
- There is a risk of more system-access breaches where personal information is accessed without a valid reason by staff working remotely, eg possibly to check friends' applications for services.
- It is easier for fraudsters to send 'urgent' emails or texts pretending to be from senior members of staff to their under-pressure teams asking for money to be transferred or for information to be disclosed.
- There is a risk of ransomware attacks. This is where malware is put into bodies' systems and leaves a ransom note demanding money in exchange for the return of information or the reinstatement of systems.
- There is a risk of an increase in **phishing** emails trying to get staff working under pressure to click on links which allow fraudsters access to public-sector systems. For example, staff receive scam emails inviting them to a video conferencing meeting, supposedly being held by someone they know and trust. The link provided leads to a fraudulent log-in page, which asks for the recipient's username and password.

### Phishing:

Where criminals send emails purporting to be from reputable sources in order to deceive individuals into providing information or data such as passwords, user names or bank details, or to click on a link that allows malware to be downloaded.



## 4. Governance

- Public-sector staff are working under extreme pressure which may mean some internal controls are suspended or relaxed.
- Existing controls may have been relaxed to assist homeworking for staff and access to services for clients.
- Fraud investigations may be paused or unable to continue due to difficulties in collecting evidence or investigation staff being redeployed to frontline services.
- When buildings are closed there are additional risks to the security and unauthorised use of assets from both internal and external sources as the removal or unauthorised use of assets may go undetected.
- New equipment and IT devices purchased during the pandemic may be at more risk of being lost or stolen due to possible weakness in controls around delivery, asset-tagging and recording in asset registers when staff are working from home. Any losses may not be detected.
- Staff may be transferred from their own departments to other areas to meet increased demand for certain services. This may leave some departments under-staffed at the same time that inexperienced staff may be working remotely without a full understanding of the required procedures and controls.
- There is a risk of weakened governance arrangements as internal audit teams are redeployed to operational areas.



## 5. Procurement

- Previous controls may be relaxed to allow bodies to buy new or existing goods or services which are required urgently, possibly from new suppliers.
- Fraudsters may be 'selling' popular and/or hard-to-get items online. The products may not arrive or may be counterfeit, eg medicines, personal protective equipment (PPE) such as face masks and gloves, and hand sanitiser products which do not provide the necessary level of protection.
- An increase in medical and sanitary waste may see criminals attempt to gain waste management contracts. This could result in the inadequate disposal of the waste, with the potential associated harm to public health as well as generating proceeds for the criminals.
- Bodies may buy goods/services from companies without due diligence and vetting being completed due to the urgent demand. This increases the risk of collusion between companies, eg bid fixing, and between companies and staff in the public body buying the goods/services.
- Bodies may receive texts or phishing emails purporting to be delivery companies saying that a parcel is awaiting delivery but that an unpaid shipping fee must be paid. The texts and emails include a link to a scam website asking for payment details.
- Bodies may also receive texts or phishing emails purporting to be from delivery companies saying that they tried to deliver a parcel to closed offices. A link is provided purporting to allow the rescheduling of the delivery. The link leads to a scam website asking for contact and payment details.



## 6. Payment

- Mandate and diversion fraud may increase as fraudsters try to get employees to update suppliers' bank details and make payments as soon as possible, knowing staff are under pressure. Some attempts may be made using a compromised email account of a genuine member of staff employed at either the public sector body or in an existing supplier.
- Due to staff working from home and under pressure, duplicate payments are possibly not detected, or payments may be made without checking whether goods and services were received to a satisfactory quality.
- Due to controls being loosened it may be possible for staff to pay invoices above their authorisation limits or without the normal approvals.
- Emails may be received from fraudsters purporting to be from a senior member of staff in a contractor requesting copies of initial contracts/award letters and previous invoices last issued. The fraudulent email may also note there has been a change in their bank account details.
- Public bodies may be contacted by someone purporting to be from the fraud department at the body's bank and advising of attempted frauds made against the body's bank accounts. The fraudster then may persuade the member of staff that they can stop the fraud by setting up a payment to a given sort code and account number.
- Messages may be received purporting to be from the bank saying that a request to add a new payee has been set up. The recipients are asked to click on a link to authorise or cancel this request. The link leads to a scam website which asks for bank account details.
- Messages may be received purporting to be from a known supplier advising that an unexpected sum of money will be debited from the body's bank account. The recipient is asked to click a link to a scam website supposedly in order to cancel the payment.
- Emails may be received where a fraudster tricks officers into thinking a message came from a person they know. For example, a staff member may receive an email from what appears to be a senior colleague requesting the purchase of gift cards and for the cards and codes to be emailed by return email, or that certain invoices have been authorised for payment.



## 7. Payroll and recruitment

- There is a risk of recruitment fraud as new staff are needed immediately due to increased demands for services and the normal checks may not be completed.
- Payroll fraud may increase as normal controls around working hours, expenses, overtime etc may be relaxed.
- Staff returning to work to help respond to Covid-19 may be targeted by unscrupulous tax avoidance schemes.
- Telephone calls may be made by fraudsters to health and social care staff requesting personal bank details in order for the £500 'thank you' payment to be made.
- Telephone calls may be received advising staff that their national insurance number has been compromised or is invalid. The caller asks for personal details in order to apply for a new national insurance number.
- Fake Covid-19 related job adverts may appear on social media, eg for Covid testers. The scammers ask for personal details that job applicants typically provide, eg bank details, proof of address and passport details. This information can be used for identity theft.
- Emails may be received purporting to be from HMRC saying the recipient is due a tax refund. The recipient is asked to click on a link to a scam website to provide personal and bank details for the supposed tax refund.

# Ways to reduce counter-fraud risks



- Discuss and agree the organisation's risk appetite and associated approach to the newly emerging risks.
- Carry out a risk assessment to identify the most vulnerable areas under the new working conditions. This will include a review of IT system security for remote working.
- Ensure Internal Audit review systems of control. Some of the existing controls are unlikely to be still relevant and appropriate.
- Introduce new systems of control to address new and emerging risks.
- Ensure existing ways of reporting fraud or irregularity are still operating and are promoted, eg fraud hotlines and whistleblowing processes are still operating.
- Review ways of working and delivering services to help ensure those in need are supported.
- Ensure staff and customers receive regular, appropriate communications on the new ways of working and changes to services.
- As staff move back to offices, controls should be reviewed to ensure they are effective and appropriate for the new ways of working. This will include possibly tightening up previously relaxed controls and carrying out audits on assets.
- Consider bank account verification and active company search services, eg that are available to the UK public sector from the Cabinet Office or **NAFN**.
- Continue staff training, especially for staff moved to work in areas that are new to them.
- Continue staff training on counter fraud including new threats. This will include updates on new and emerging frauds as well as reminders that suspicious activity still needs to be reported.
- Run 'dummy phishing' exercises to test employees' reactions, with a requirement to revisit training modules if an employee 'fails'.
- Ensure all software updates are applied as soon as possible to IT systems. This includes regular reviews and updates to all systems and devices and actively looking for vulnerabilities. Where dangerous vulnerabilities are identified, system updates are done immediately even if it means staff can't work while it is being updated. Where a device, eg a laptop, isn't updated, it is disabled and excluded from the network.
- Block and filter every attack vector possible, which can make things difficult for colleagues, and say no to anything that could increase the organisation's susceptibility to attack.

## NAFN:

Shared service organisation open to all public-sector organisations. NAFN provides data, intelligence and best practice services for member organisations.



# Ways to reduce counter-fraud risks



- Review **NFI** matches to identify fraud and error or system control weaknesses.
- Rotate employees or volunteers working with vulnerable service users and ensure appropriate employee disclosures are up to date.
- Review the NHS Counter Fraud Authority's guidance including the [Covid-19 counter fraud guidance](#)
- Review the UK Government Counter Fraud Function's website for the latest guidance including:
  - [Covid-19 Counter fraud response team](#)
  - [Fraud Control in Emergency Management: Covid-19 UK Government Guidance](#)

## NFI:

National Fraud Initiative, an exercise that matches electronic data within and between public and private-sector bodies to prevent and detect fraud.

Further information:

### **The National Fraud Initiative in Scotland 2018/19**

July 2020



# A focus on procurement risks



Procurement fraud in the UK is not defined but industry experts put the figure at billions of pounds a year. Procurement fraud is complex and covers a wide range of activities from the pre-contract award phase through to the post-contract phase. Procurement fraud is difficult to detect. Although data analytics to identify fraud are on the increase, manual detection techniques are an important part of fraud prevention approaches.

In order to help reduce some of the risks around procurement, bodies may consider the following:

- All staff should be aware of the potential red flags to look out for within any procurement exercise.
- All staff involved in procurement activity should receive regular appropriate training to help them to identify fraud and error.
- There should be clear processes, procedures and controls to be followed regarding procurement. Checks should be made, eg by internal audit, to ensure these are followed.
- A central contract register should be in place which is regularly reviewed and analysed for irregularities.
- Staff should be extra vigilant where a contract is required in a rush and/or where the contractor may be pressurising staff for a quick response.
- Appropriate controls should be in place to ensure invoices, purchase orders and requisitions all agree before payments are made.
- Appropriate segregation of duties should be in place for the authorisation of contracts, payments and technical specifications.
- Procedures should be in place and followed, for all requests for payments to new bank account details.
- Due diligence should be carried out on new suppliers. This may include a review of online customer reviews, and calling the landline on a website to check it is genuine.
- Consideration should be given to job rotation to ensure staff do not deal with the same clients on a long-term basis.
- Internal audit should review procurement activity, eg through spending analysis, to identify where any large spend to a particular supplier may exceed approval thresholds when aggregated or a review of the security around bids and tender documentation.

Further information:

## Red flags Procurement

October 2019



# Fraud and irregularity identified during 2020/21



Auditors have provided Audit Scotland with details of cases of fraud and other irregularity discovered in their audited bodies during 2020/21. This report sets out examples of the various different categories of fraud and irregularity reported during 2020/21 and the control weaknesses which have contributed to these cases.

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.

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.

Auditors should confirm that appropriate governance arrangements for the prevention and detection of fraud are in place at their audit clients and that appropriate reviews and amendments of controls have taken place in response to new ways of working. They should also confirm whether internal controls are sufficiently strong to prevent the types of frauds and errors highlighted in this report.

## Fraud and irregularity reported during 2020/21 totals £0.4 million

Falls into the following key categories:



**2**

cyber attacks



**5 cases = £132,500**

Fraud and irregularity involving expenditure



**4 cases = £25,000**

Fraud involving payroll



**1 case = £237,000**

Theft



**1 case = £7,000**

Involving third party funds

Control weaknesses were highlighted where fraud or irregularity was identified.

# Common control weaknesses

A review of fraudulent and irregular activity highlights common control weaknesses which have contributed to the fraudulent and irregular activity reported by external auditors.



A lack of management checking and review



Procedures not followed



Weak security arrangements



A lack of staff training



Missing indicators within emails that the email is not genuine



Not verifying applications for funding to existing records



Poor budget monitoring



System reconciliation weaknesses



Poor record keeping

# Cyber attacks

A cyber attack is where computers and networks are targeted by criminals in order to alter, disable, steal or gain information through the unauthorised access to computer systems. Our blog entitled '[Cybercrime is a risk that the public sector in Scotland needs to take seriously](#),' raises awareness among boards and non-executive directors of this growing area of risk as well as to signpost readers to key resources to help protect organisations from this type of crime.

## Case study 1

**A public body was subject to a serious complex cyber attack which impacted upon access to systems, processes and communications.**

### Key features

1.2GB of data amounting to just over 4,000 files had been stolen.

The public body instigated its business continuity plan and took action to limit the impact of the attack. The public body made clear that it would not engage with criminals intent on disrupting public services and extorting public funds.

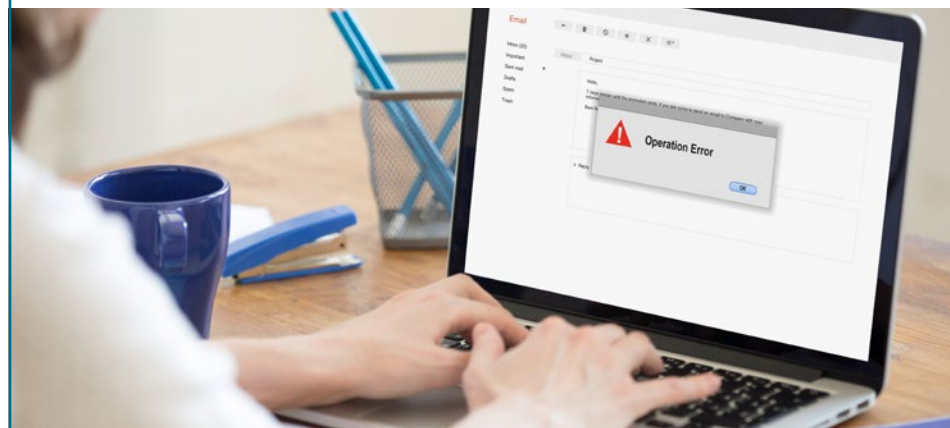
The information that was stolen from the public body's systems was published illegally online on the dark web the following month. The information that was published is still being assessed. IT systems have been disconnected to prevent further data losses.

The impact of this attack will last for some time due to the loss of data, including financial data, and the need to re-build systems and re-create records.

A Police Scotland investigation is under way. The public body is also working with the Scottish Government, the Information Commissioner and the National Cyber Security Centre in order to investigate the specific details of the attack and identify areas to strengthen existing controls.

## Case study 2

**A cyber-attack caused disruption to services at several colleges.**



### Key features

The colleges' IT engineers worked to isolate and minimise the impact from the incident.

As a result of the attack, the colleges were closed to some students for a short period of time.

The source of the attack is not known, however a Police Scotland investigation is currently under way.

# Expenditure

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.

## Case study 3: Invalid supplier

A third party defrauded over £46,000 from a public body by purporting first to be a staff member and then a supplier to the body.

### Key features

One of the public body's suppliers received an email purporting to be from the body, asking if there were any outstanding invoices. The supplier replied attaching an invoice. The public body then received an email purporting to be from the supplier with the invoice attached asking for it to be paid to a new bank account. The bank records were amended, and the invoice paid. The fraud was identified when the genuine supplier contacted the body looking for payment of the invoice.

The fraud was possible as:

- the accounts payable department did not confirm that the change of bank details had been verified by the contracting service
- the member of staff within the contracting service had not received training on how to verify new bank details
- indications within the email that it was not genuine were missed
- learning from a previous unsuccessful similar attempted fraud involving the same supplier had not been shared with staff.

The public body is introducing robust verification processes for change of bank details.

## Case study 4: Invalid supplier (2)

A third party defrauded £64,500 from a public sector body by purporting to be a genuine supplier.

### Key features

The purchase ledger team received several emails purporting to be from a named contact at their utility supply company requesting payment of legitimate outstanding invoices. They included copy invoices from the supplier which appeared to be genuine. The emails requested that the standing bank details be amended to those on the invoices. The bank details were changed, and three payments were made. Remittance advices were sent to the legitimate supplier's email address. The fraud was identified when correspondence was received from the legitimate supplier advising that they had received remittance advice notices but no payment.

The fraud was possible as the procedure for confirming bank account changes was not followed. In addition, the email from the supplier had a subtle difference in the address that was not identified at the time.

All finance staff are now receiving training on fraud prevention and detection. The body has notified Police Scotland.

# Expenditure

(continued)

## Case study 5: Misuse of a vehicle

A public sector employee defrauded almost £7,000 through unauthorised use of a car over a six-month period.



### Key features

The employee was using a hire car while at the same time using a leased car. Both cars were provided by their employer.

The fraud was identified after the payroll team questioned why the car was still on hire.

The fraud was possible due to a lack of review and challenge by the line manager of the monthly car hire report for their department.

The case has been reported to Police Scotland and options for civil recovery are being investigated.

## Case study 6: Misuse of vehicle

A public sector employee defrauded over £5,000 over an eight-month period through unauthorised use of a car.



### Key features

The employee used a pool car for personal use after their own car broke down.

The fraud was identified after a finance report was issued to the budget holder suggesting that providing the employee with a small van would provide better value for money.

The fraud was possible as the budget holder failed to identify the pool car recharges and investigate accordingly.

Internal audit has reviewed the pool car system to identify system weaknesses.



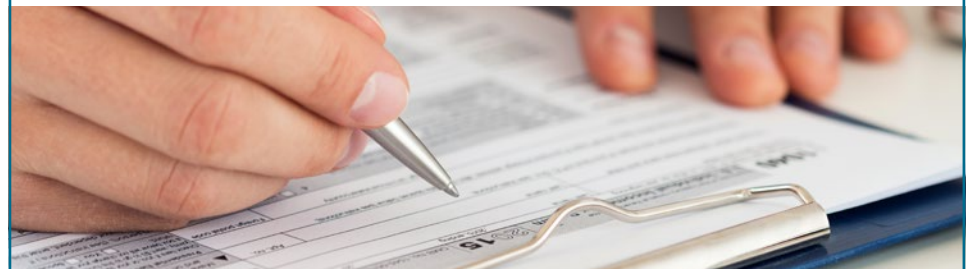
# Expenditure

(continued)

Public bodies have been issuing many different grant and funding streams to businesses and individuals over the last year due to the Covid-19 pandemic. There have been many instances of claimant fraud identified in these applications. This report does not include cases of fraud that are perpetrated by claimants, for example, grant claims, unless the fraud was facilitated by either the collusion of local authority staff or by weaknesses in internal control.

## Case study 7: Grant payment

A third party defrauded £10,000 from a council by making a false claim for a business grant.



### Key features

The perpetrator claimed a business grant for premises they had previously occupied. The fraud was identified when the legitimate business proprietor applied for a grant.

The fraudulent payment was possible as the council failed to identify that:

- the name on the business grant application was not the name of the business on the business rates system
- the bank statement used in support of the application was for a personal bank account rather than a business bank account.

Internal controls have been improved and more stringent checks are now carried out.



# Payroll

Payroll frauds relate to cases where an organisation's payroll has been misappropriated, eg employees working elsewhere while claiming to be unfit or where salary payments have been redirected.

## Case study 8: Re-directing salary

Four parties defrauded almost £25,000 from four public bodies by redirecting salary payments.



### Key features

In all cases, the payroll team received emails purporting to be from genuine members of staff, advising of a change to be made to bank account details. The payroll records were amended, and salary payments were made. The frauds were identified when employees contacted the payroll team to query why they had not been paid.

The fraud was possible as the procedures in place to check the validity of bank detail changes had not been followed.

Payroll staff have been reminded of the proper procedures, including verification procedures for changes to employee bank account details. The cases have been referred to Police Scotland for investigation.

# Theft of assets

Theft relates to cases where someone acts dishonestly appropriating property belonging to another with the intention of permanently depriving the other of it.

## Case study 9: Theft of assets and cash

An employee misappropriated cash and other assets valued at £237,000 from a public body over a period of eight years.



### Key features

The employee was responsible for maintaining records for a secure store. The employee abused their position of trust.

The theft was possible due to inadequacies in the reconciliation of a manual card recording system and in management oversight. The theft was identified when a new process for recording the cash and other assets was introduced and the perpetrator was going to be moved to a new department.

A subsequent internal audit identified the cash and assets were missing. Police Scotland were informed.

The employee admitted the theft, was prosecuted and imprisoned for over three years.

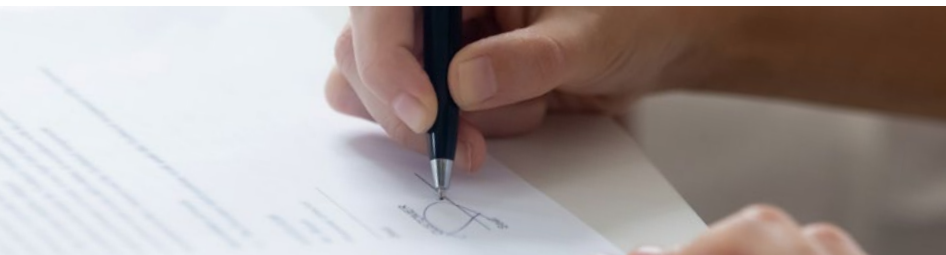
Procedures have been reviewed and improvements made.

# Private funds

Private fund frauds relate to cases where third party's funds have been misappropriated.

## Case study 10: Third party funds

A member of staff misappropriated over £7,000 from the accounts of vulnerable social care clients.



### Key features

The member of staff committed the fraud by forging the signature of another staff member. The fraud was identified when a colleague examined records of client funds and identified an entry that they had apparently authorised but had no knowledge of.

When interviewed, the member of staff admitted forging the signature of a colleague. An internal audit identified the full extent of the fraud.

The fraud was possible due to weakness in record keeping and in the oversight by management and the **Corporate Appointee**. Improvements have been introduced in relation to reconciliation processes and the review of client accounts.

The matter was reported to Police Scotland and disciplinary processes were instigated. The member of staff has repaid the full amount.

### Corporate Appointee:

A Corporate Appointee is where an organisation, eg a council, has been appointed by the DWP to manage and look after a customer's welfare benefits to make sure they get the benefits they are entitled to.

# Next steps for governance boards in scrutinising counter-fraud arrangements

## Strategies



- ✓ Are there appropriate and up to date counter-fraud strategies in place?
- ✓ Are there appropriate governance and oversight arrangements for the counter-fraud strategies? This will include appropriate performance reporting arrangements.

## Risk assessment



- ✓ Has an assessment been carried out of where the fraud and error risks lie?
- ✓ Has the risk from fraud and error risk been measured and reported? This should be updated regularly.
- ✓ Have controls been put in place to prevent and detect these risks?

## Controls review



- ✓ Are the controls regularly reviewed to ensure they are operating effectively and still appropriate?
- ✓ Are controls amended or new controls implemented where new risks emerge?

# Further information

You can find further information about Audit Scotland's work to support counter-fraud and good governance 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**



Report:

**How councils can safeguard public money**

April 2019



Blog:

**Cybercrime: A serious risk to Scotland's public sector**

May 2021

# Fraud and irregularity 2020/21

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](http://www.audit-scotland.gov.uk/accessibility)



Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN  
T: 0131 625 1500 E: [info@audit-scotland.gov.uk](mailto:info@audit-scotland.gov.uk)  
[www.audit-scotland.gov.uk](http://www.audit-scotland.gov.uk)

ISBN 978 1 913287 55 9