Public sector fraud risks



AUDIT SCOTLAND

Prepared by Audit Scotland
19 November 2026

Contents

Key messages	3
Introduction	4
Procurement	6
Bank mandate	8
Staff	10
Conclusion	13
Other resources	14

Accessibility

You can find out more and read this report using assistive technology on our website www.audit.scot/accessibility.

Key messages

1. Procurement, bank mandate fraud and staff fraud are the most significant fraud risks currently being identified across Scottish public bodies.
2. Financial pressures and reduced staffing are increasing control weaknesses.
3. Auditors continue to identify weaknesses in segregation of duties, reconciliations and oversight.
4. Public bodies should assess their exposure to the risks highlighted in this report and review the effectiveness of their controls.
5. Auditors should consider these risk areas when planning and performing audit work.

Introduction

Aims of this report

1. This report from Audit Scotland shares information where control weaknesses may contribute to fraud and irregularity. This report aims to help prevent similar situations happening in other bodies by sharing the examples of frauds found and highlighting weaknesses in internal controls.

2. This report encourages public bodies to consider the examples included in this report and reflect whether the same control weaknesses exist in their own systems. Public bodies are also encouraged to regularly review their counter-fraud arrangements to ensure they remain effective against both existing and newly emerging types of fraud and irregularity.

3. The examples in this report also aim to help auditors consider and review the effectiveness of the counter-fraud governance arrangements in their audited bodies.

Background

4. Public sector bodies are responsible for having systems and processes in place to safeguard public money and deter fraud. That does not always mean that procedures cannot break down, are not kept up-to-date or that people will not try to find ways to circumvent the system for personal gain.

5. With public sector bodies under severe financial pressure, this can lead to situations where fewer staff have more responsibilities and less time to carry out checks. This can cause a lack of segregation of duties, insufficient oversight and review, reconciliations not being undertaken and budgetary control weaknesses. Without these internal controls operating effectively, public sector bodies may struggle to prevent, deter and detect fraudulent activity.

6. This report focuses on three high risk areas (set out at Exhibit 1) where fraudulent activity may occur in public sector bodies. Links to other available resources are provided.

Exhibit 1 Key Fraud risk areas

Procurement

Procurement activity often involves complex processes, multiple stakeholders and third-party relationships, creating opportunities for collusion, conflicts of interest, manipulation of tendering processes, bribery and fraud. Financial pressures, resource constraints and weaknesses in oversight can further increase the risk of fraud.

Bank mandate

Bank mandate fraud has developed from a manual fraudulent activity where the fraudster sent in a forged letter to the targeted body to become much more complex with the use of technology and hacking. This type of fraud is attractive to fraudsters as it can be carried out remotely.

Staff

Staff fraud can arise in many forms and remains a significant risk for organisations. In recent years, this risk has been heightened by ongoing cost-of-living challenges and pressures on staffing resources within public sector bodies.

Procurement

7. Procurement can be an attractive area for fraudsters as it involves complex processes which are lengthy, involved, and often, high value contracts. Due to the high risk of fraud, NHS Scotland has identified procurement as a strategic priority area in its Counter Fraud Strategy 2026-29. Some high-profile cases have occurred in Scottish bodies such as:

- a £6 million NHS contract fraud
- a £3 million fraud in The University of Edinburgh regarding false and over-inflated invoices
- procurement breaches in Forth Valley College

8. Procurement weaknesses have been reported in public sector bodies including the replacement of new ferries for the Clyde and Hebrides and in Historic Environment Scotland.

9. Audit Scotland previously issued a report in 2019 detailing the Red Flags in Procurement. The report set out some red flags to help identify circumstances which may indicate the need for further audit work.

Risk areas

10. This report highlights some of the key risks relating to procurement activity as shown in Exhibit 2.

Exhibit 2
Risks that may lead to procurement fraud

Area	Indicators and warning signs
Collusion either between contractors or between procurer and bidders	One officer has sole control of the tender process
	Significant expenditure incurred through multiple low-value contracts approved under delegated authority, suggesting contract splitting, collusion, or avoidance of procurement controls
	The bidder offers gifts to the procurer
	Officers involved in procurement have a relationship with the bidder

Area	Indicators and warning signs
	One supplier wins many bids
	Submission of fictitious bids to give appearance of competition
	All bids appear expensive may indicate bid fixing
	Bidders don't declare connections with other bidders.
	One supplier is favoured
Pre-tender	A lack of evidence that the good/service is required
	Breaking the procurement into smaller lots to circumvent approval/tender thresholds
Tender bids	Altering bids
	Accepting late bids
	Manipulation of tender scoring process
Contracts	No/inadequate checks on work performed before paying invoices
	Invoices do not match contract
	Design of contracts leave them open to manipulation
Payments	VAT charged on invoices but not VAT registration number
	Duplicate or inflated invoices
	The same person is responsible for both signing off and paying invoices.

Source: Audit Scotland

What should public bodies do now?

- Ensure segregation of duties exists throughout tendering and payment processes
- Complete and review conflicts of interest declarations
- Monitor procurement thresholds
- Use data analytics to identify unusual supplier patterns
- Actively reviewed gifts and hospitality registers

Bank mandate

11. Bank mandate fraud occurs when a fraudster changes a supplier's, customer's, employee's, or organisation's bank account details without proper authorisation, resulting in legitimate payments being redirected into an account controlled by the fraudster. The fraud is often facilitated through phishing emails, business email compromise, social engineering, or the interception of genuine correspondence, allowing the fraudster to impersonate a trusted party and request amendments to banking information.

12. Bank mandate fraud remains a highly attractive fraud type due to the potentially significant financial gains that can be achieved through a single successful attack. Public sector bodies process large volumes of payments and often rely on electronic communication and automated payment systems, creating opportunities for fraudsters to exploit weaknesses in verification controls. Fraudsters frequently target changes to supplier bank details because these requests may appear routine and therefore attract less scrutiny.

13. The fraud can be difficult to detect at the point of payment, as transactions are usually authorised through established payment processes and directed to what appears to be a legitimate supplier account. By the time the fraud is identified, funds may have been quickly transferred through multiple accounts, reducing the likelihood of recovery.

14. Recent Scottish public sector examples include fraudsters:

- impersonating a supplier and being paid £13,000 to a fraudulent bank account
- obtaining £34,000 by impersonating a foreign supplier
- compromising a supplier’s email account and being paid £5,000.

Risk areas

15. Some key risks relating to bank mandate fraud are shown in Exhibit 3.

Exhibit 3
Risks that may lead to bank mandate fraud

Area	Indicators and warning signs
Bank detail changes	Lack of independent verification of bank account amendments before payments are processed
	Minor changes to email addresses that may be due to impersonation
	Urgent requests for payments to a new bank account
	Changes requested by individuals not previously involved in supplier communications
	Requests to change a supplier's bank account details received only by email.

What should public bodies do now?

- Independently verify all bank detail changes
- Use trusted contact details to complete verification
- Secondary approval for high-risk amendments
- Ensure staff receive regular phishing awareness training

Staff

16. Staff fraud can take various forms, including payroll fraud, theft of cash or assets, making unauthorised payments, recruitment fraud and abuse of position. Such fraud is often enabled by an employee's access to organisational systems, funds, assets, and sensitive information, allowing them to exploit weaknesses in internal controls for personal gain.

17. While most employees act with integrity, insider fraud presents a significant risk to public sector bodies due to the potential for financial loss, service disruption, reputational damage, and erosion of public trust. Strong governance, monitoring, and fraud prevention controls are essential.

18. Recent Scottish public sector examples include:

- A Dundee City Council employee embezzled £1.065 million by inserting fake invoices into the system and altering supplier bank payment details to their own bank account details.
- An Aberdeen City Council employee fraudulently transferred £1.1 million of council tax refunds to his own bank account.
- The recent National Fraud Initiative (NFI) report published in August 2026 identified
  - two cases of dual full-time working (holding more than one full-time job), with three potential cases still under investigation.
  - three cases of employees working in a secondary role while off sick from the main employer with a further five potential cases still under investigation.
- A public sector employee misappropriated £27,000 of client money.
- An employee failed to notify their employer of £20,000 of income they were not entitled to as they were not working.
- An employee authorised their own shift work to the value of £15,000. It is uncertain whether the employee worked all 49 shifts as records show login activity for only six shifts.
- An employee spent £500,000 of her employer's money on electronic devices which she then sold.
- Several examples of NHS workers taking medical equipment worth £1.3 million, £75,000 and £23,000.

Risk areas

19. Some of the key risks relating to staff fraud are shown in Exhibit 4.

Exhibit 4
Risks that may lead to staff fraud

Area	Indicators and warning signs
Procurement card fraud	Cards issued without clear business justification Inadequate transaction reviews Weak receipt checking Delayed review of card statements
Payroll fraud	Inadequate segregation of duties between HR and payroll Lack of independent review of payroll changes Failure to promptly remove leavers from payroll Insufficient monitoring of overtime and allowances Absence of periodic payroll reconciliations
Expense claim fraud	Claims approved without supporting documentation Excessive reliance on manual processes Inadequate managerial scrutiny Lack of data analytics to identify duplicate/unusual claims Weak expense policies
Supplier payment fraud	Inadequate approval controls Insufficient segregation between supplier creation and payment authorisation Failure to monitor unusual payment activity.
Fictitious supplier fraud	Weak supplier onboarding processes Absence of supplier validation checks Inadequate monitoring of one-off suppliers Poor review of supplier master data
Asset misappropriation	Poor asset tracking Inadequate inventory management Infrequent stock checks Lack of physical security measures Weak controls over asset disposal and write-off processes

Area	Indicators and warning signs
Cash theft	Poor segregation of collection, recording, and banking responsibilities Inadequate supervision of cash handling activities Insufficient income reconciliation Lack of surprise checks and independent reviews
Funding fraud	Weak verification of eligibility criteria Inadequate review of supporting evidence Poor monitoring of grant payments Insufficient oversight of approvals Limited post-award assurance activity
Recruitment fraud	Lack of independent oversight of recruitment decisions Inadequate pre-employment screening Absence of conflict-of-interest declarations Poor documentation of recruitment decisions Insufficient challenge of appointments
Conflict of interest and abuse of position	Weak declarations process Failure to maintain registers of interests, gifts and hospitality Poor management oversight Lack of training Inadequate review of decision-making activity

What should public bodies do now?

- Promote whistleblowing arrangements and a strong ethical culture
- Provide regular fraud awareness training
- Maintain effective segregation of duties.
- Use data analytics and exception reporting to identify unusual activity.
- Investigate concerns and control weaknesses promptly.

Conclusion

What good looks like

20. Fraud risks continue to evolve, particularly where financial pressures, workforce challenges and increasing digitalisation weaken existing controls. Public bodies should regularly review their fraud risk assessments, while auditors should remain alert to indicators of control failure in high-risk areas such as procurement, bank mandate changes and staff-related fraud.

21. Organisations with effective fraud prevention arrangements typically:

- Maintain an up-to-date fraud strategy.
- Conduct periodic fraud risk assessments.
- Use internal audit and other assurance functions to provide independent review of fraud risks, controls and emerging indicators of irregularity.
- Use data analytics to identify anomalies.
- Train staff regularly.
- Encourage whistleblowing.
- Review fraud incidents and lessons learned.

Other resources

Audit Scotland's report on Red Flags, Procurement.

The Competition and Markets Authority have detailed information and a free e-Learning module which covers anti-competitive practices in procurement.

Skills Development Scotland have prepared a Conflicts of interest in Procurement Best Practice Guidance note.

The Public Sector Fraud Authority has published a practice note on the Bid-Rigging Risk in Procurement.

NHS Scotland National Services Scotland Bank Mandate fraud

NHS Counter Fraud Authority's Invoice and Mandate Fraud guidance

Police Scotland Direct Debit Fraud guidance

The NAFN, Action Fraud and Police Scotland Bank Mandate Fraud Guidance Document

NHS National Services Scotland's Insider Threat-Managing people securely

The National Protective Security Authority's Insider Riak Mitigation Framework

CiFAS The silent fraud- tackling the growing issue of the insider threat in the Public Sector

Public sector fraud risks

Audit Scotland, 4th Floor, 102 West Port, Edinburgh EH3 9DN
Phone: 0131 625 1500
www.audit.scot

AS.5.0