The 2016/17 audit of Dundee City Council

Report on a Significant Fraud

ACCOUNTS COMMISSION

Prepared for the Accounts Commission
Made under section 102(1) of the Local Government (Scotland) Act 1973
February 2018

Audit Scotland is a statutory body set up in April 2000 under the Public Finance and Accountability (Scotland) Act 2000. We help the Auditor General for Scotland and the Accounts Commission check that organisations spending public money use it properly, efficiently and effectively.

Contents

Executive Summary

Introduction

1. The external auditor's report on the 2016/17 audit refers to a significant fraud perpetrated against Dundee City Council. The fraud was complex and resulted in a long term employee embezzling £1.065 million from the council between August 2009 and May 2016. I submit this report under section 102(1) of the Local Government (Scotland) Act 1973 as a matter that the Controller of Audit considers should be considered by the local authority or brought to the attention of the public.

2. The purpose of this report is to draw the Accounts Commission's attention to how the fraud was perpetrated; the weaknesses in the council's control systems; and the actions taken by the council following discovery of the fraud. The financial loss to the council and the recovery outcome are also reported.

Summary

3. During routine year end procedures the council highlighted an invoice for £7,337 where supporting information could not be found. The payment for this invoice was made into an employee's bank account in May 2016 which resulted in an internal investigation and a Police Scotland investigation. The reviews highlighted fundamental weaknesses in the council's internal financial control systems. Investigations identified fraudulent payments to the employee totalling £1,065,085 during the period from August 2009 to May 2016.

4. The fraud resulted from the employee having unrestricted access to several systems which allowed him to insert fake invoices into the system and alter the bank payment details of suppliers without detection.

5. The employee was immediately suspended and resigned from his position in June 2016. The Police Scotland investigation resulted in the ex-employee pleading guilty on 2 August 2017 to the charge of embezzling £1,065,085 from the council and on 24 August 2017 at the High Court in Glasgow he was sentenced to 5 years 4 months imprisonment.

6. Full recovery of the loss, excluding the policy excess of £10,000 and fees of £8,663, has been achieved through a range of methods. The recovery included the pension of the convicted individual, an ex gratia payment from a third party and the proceeds of the council's fidelity insurance policy.

7. PricewaterhouseCoopers (PwC) provided additional specialist support, under their internal audit contract, for the investigation. The PwC reports issued to management in October 2016 and June 2017 highlighted control weaknesses; recommendations for improvement; and details of reviews undertaken to ensure no further anomalous payments were made.

8. The Leader of the Council, Depute Leader and Group Secretary were provided with details of the fraud in June 2016. During 2016 the Chair of the Scrutiny Committee and other senior

politicians were briefed on the fraud and the actions being taken. Member briefings on the fraud were provided by management on 19 April and 5 December 2017 with a report considered by the Scrutiny Committee on 13 December 2017. The Scrutiny Committee report indicated that all the PwC recommendations had been implemented or had an agreed implementation date.

9. Internal audit's plan for 2018/19 are to include following up the PwC recommendations to ensure that these have been implemented effectively. Internal audit as part of the current year have planned to review the Bank Automated Clearance System (BACS) and User Access Levels to provide further assurance to members for these areas.

Auditor's opinion

10. The fraudulent payments totalled £1.065 million over several years and the impact on the financial statements from 2009/10 to 2015/16 did not represent a material misstatement in any given year. However, there were failures in fundamental controls within the council that allowed this fraud to continue over a prolonged period resulting in a loss to the council. In particular, the lack of segregation of duties allowed the perpetrator access to a number of systems, enabling them to carry out the fraud. Internal controls such as system reconciliations were not carried out or were ineffective and as a result the payments were not identified as anomalies for further investigation at an early stage.

11. On discovery of the erroneous payment the council acted promptly to deal with the individual and reporting the fraud to Police Scotland. Officers undertook appropriate investigations and effective recovery of the fraudulent payments. The investigations highlighted the control weaknesses and officers have acted to address the issues and strengthen the control environment.

12. Elected members and the local external audit team have been kept up to date at appropriate key stages of the fraud investigations since its discovery.

13. Members' briefings were held in April and December 2017 and a report was also presented to the Scrutiny Committee on 13th December 2017. External audit was invited and attended these meetings and considered them comprehensive and informative.

14. The council continues to strengthen its control environment through its Corporate Integrity Group, which was established in February 2017. Police Scotland has also approached the council in order to develop a case study of the fraud to provide a resilience message across Scotland's public sector.

15. The wider lesson from this incident, for other councils to consider, is the importance of key internal controls. These are documented in Appendix C and cover areas such as: segregation of duties (including user access rights); effective system reconciliations; system documentation; and effective budget monitoring.

Fraud details

Initial discovery and quantification

16. On 20 May 2016, as part of the council's year end procedures, an invoice for £7,337 was highlighted where supporting information could not be found. A request was made on 23 May to the IT helpdesk to investigate the issue. On 25 May the IT officer investigating the issue (the perpetrator of the fraud) highlighted that he had been carrying out testing of the BACS system and had used his own bank details to test a payment. The employee immediately returned the payment of £7,337 to the council. Finance staff notified senior management and it was agreed that the employee should be suspended with immediate effect to allow for a full investigation to be undertaken. The employee was suspended on 26 May 2016 and Police Scotland notified on 30 May.

17. At the same time a further query on a fleet management invoice by council staff for an invoice of £17,846 highlighted a second bank account, suspected to be controlled by the employee.

18. A formal disciplinary meeting was held with the employee on 9 June 2016, solely in relation to the payment of the initial £7,337 discovered. At the meeting, prior to being issued with a notice of dismissal, the employee tendered his resignation.

19. In June 2016 PwC were requested to provide additional support for the investigation through an existing internal audit contract to:

- establish the extent of any anomalous payments and where these are posted in the accounting records
- establish where failings in the current control environment enabled the fraud to be perpetrated without detection
- identify improvements to the control environment that would help prevent similar incidents in future
- assess the resilience of the council's systems to external threats.

20. Interrogation of the BACS system by PwC verified £804,775 of fraudulent payments, 44 made to the employee's personal account dating from March 2012 totalling £786,929 and 1 of £17,846 made to a second bank account. The BACS system was upgraded in March 2012 and the council was unable to establish whether payments had been made to these accounts prior to the system change.

21. Police Scotland's investigation subsequently identified an additional 12 fraudulent transactions totalling £260,310 between August 2009 and July 2012.

22. From August 2009 to May 2016 the fraud totalled £1,065,085 resulting from 57 transactions with payments to two bank accounts. These accounts were different accounts from where the employee's salary was paid into.

23. The employee was charged and convicted with regard to the fraud and is currently serving five years in prison.

Financial loss to the council

24. The council has insurance cover (Fidelity guarantee) to protect itself against dishonesty of employees resulting in financial loss to the authority. Following discovery of the fraud, a formal claim was submitted with the insurer appointing an independent loss adjuster to investigate the claim.

25. The council has recovered all of the loss from the fraud excluding the policy excess of £10,000. The recovery methods included the pension of the convicted individual, an ex gratia payment through a third party and the proceeds of the fidelity insurance policy. The recovery also covered £47,141 towards the PwC fees of £55,804 for their investigation.

How the fraud was perpetrated

26. The employee was an IT officer with over 30 years' service, who had extensive access to a large number of the council's financial systems which had been built up over many years.

27. The employee combined his knowledge of the systems, and his system access privileges, to insert fake invoices into the purchase ledger for payment. These invoices appeared to have come through an interface from a sub-system and were payable to known suppliers. The sub-systems did not record these transactions.

28. Further to this, the employee was able to intercept these fake invoices and divert payments to bank accounts within the individual's control. A genuine payment to the same supplier would not be intercepted, resulting in suppliers being paid as normal.

Why budgetary control processes did not detect the fraud

29. Prior to 2012 the council is unable to assess the quality of its control environment as no audit trail has been retained by the council prior to this period. The 45 fraudulent transactions totalling £804,775 that the council is able to access were processed through two systems (29 payments through the construction sub-system totalling £501,407; and 16 payments through the fleet management sub-system totalling £303,368).

30. The construction sub-system is a bespoke system developed in-house in the 1980s. The employee who committed the fraud, was involved in the development and has extensive knowledge of this sub-system. Interfaces from the construction sub-system enter the council's ledger as a batch total split across cost centres rather than on an invoice by invoice basis.

31. The fraudulent transactions were not recorded in the sub-system and the fake interface of these transactions to the purchase ledger resulted in them being split across various cost centres.

32. A review of the construction sub-system would therefore not contain any fraudulent transactions and a review of the general ledger would not allow budget holders to dig down to

individual invoices to investigate variances. As the fraudulent payments were for small amounts between £5,898 and £27,557 over a number of years they did not stand out in the high value and volume of genuine transactions processed through the construction sub-system. Budget monitoring did not, therefore, identify any of the fraudulent payments.

33. The fleet management system is an "off the shelf" system widely used in the private and public sector. The council's ledger for these areas should have been subject to regular management review and would have allowed analysis down to invoice level. One of the fraudulent payments (£17,846 highlighted above) was queried however it is unclear why the remaining payments went undetected by budget holders although the volatility of fuel prices may have helped mask the impact of these payments.

Control weaknesses that facilitated the fraud

34. The PwC report *Phase 1* was issued to management in October 2016. The report highlighted a number of fundamental control failings that enabled the fraudulent payments to go undetected and resulted in key areas for control improvement (Appendix A) in relation to:

- **segregation of duties:** The employee had unrestricted access to a number of key systems across the purchase to payable cycle that allowed the insertion of fictitious invoices and malicious code into interfaces and the BACS payment system.
- **interface reconciliations**: Interface reconciliations were ineffective. An effective interface reconciliation of the number and value of transactions interfaced may have allowed for earlier detection of the fraudulent activity.
- **balance sheet reconciliations**: A reconciliation of the fleet management system to the general ledger was not undertaken. The limitations in the construction sub-system resulted in the reconciliation for the construction system to the general ledger being an ineffective control.
- **supplier statement reconciliations**: The council had not conducted supplier statement reconciliations to supplier's accounts that would have highlighted the fake invoices.
- **system limitation**: Limitations on the construction sub-system had a pervasive impact across the control environment, undermining the effective operation of segregation of duties, interface, and balance sheet reconciliation controls. This was exacerbated by the lack of system and process documentation which articulate the flow of transactions and sets out how interfaces work. The system is viewed by management as no longer fit for purpose and is scheduled to be replaced in 2018.

35. A further PwC review was agreed in December 2016 with the scope to:

- review the control environment over the Construction purchase-to-pay process to identify gaps and/or weaknesses and design appropriate controls to mitigate these
- review the existing reconciliations performed between the Construction sub-system and the council's general ledger to identify and design improvements in the reconciliation process

36. The PwC report *Phase 2* was issued to management in June 2017 and highlighted additional improvements surrounding the construction IT system and included:
    - journal, reconciliation and interface controls
    - process improvements for journal entries for construction invoices
    - construction system and civica reconciliations
    - segregation of duties within IT
    - super-user/administrative passwords.

Informing the elected members of the fraud

37. The Leader of the Council, Depute Leader and Group Secretary were informed of the fraud through discussions with the Chief Executive and Executive Director of Corporate Services on 13 June 2016. During 2016 the Chair of the Scrutiny Committee and other senior politicians were briefed on the fraud and the actions being taken. No formal documented briefings were presented to members during this time as investigations which were part of disciplinary and police investigations were ongoing. The external auditor has been kept well informed since the discovery of the fraud.

38. Scrutiny Committee members were invited to a briefing in April 2017 and all elected members were invited to attend briefings on the fraud in December 2017. These briefings were also attended by the external audit team who considered them comprehensive and informative.

39. The report to the Scrutiny Committee in December 2017 summarised the above actions and findings from the PwC reports. The reports indicated that all the PwC recommendations had been implemented with the exception of system and process documentation which is nearing completion and is linked with the implementation of the new construction system which is planned to go live in August 2018.

Data analytics

40. To provide assurance to the council that no further fraudulent transactions were processed in a similar manner, in other systems, PwC used data analytics to scan for any anomalous payments:
    - identifying suppliers with BACS payments to more than one bank account
    - comparing payment files in the purchase ledger and the BACS system
    - matching invoices in the construction sub-system with those in the general ledger
    - matching invoices in the fleet management system with those in the general ledger

41. The testing did not identify any further fraudulent payments. The testing in this area was restricted to the back-up information retained by the council (e.g. PwC highlighted that only 76.5% of payment files have survived for the analysis of the post 2012 BACS payments). Due to system limitations it was also not possible to run effective analytical tests on payments made through the pre 2012 BACS system.

Internal audit

42. The 2017/18 Internal audit plan agreed by the Scrutiny Committee in April 2017 contains planned reviews of BACS and User Access Levels to provide assurance to members and management around the control environments in these areas.

43. As part of the 2018/19 internal audit plan, resources will be set aside to follow-up on all recommendations made in the PwC report to ensure these have been implemented as intended. A report on the findings from that review will be submitted to the Scrutiny Committee in line with standard reporting procedures.

Further council action

44. The council continues to try to enhance public confidence and improve the organisation's resilience to fraud and corruption, through its Corporate Integrity Group, which had been established in February 2017 and is chaired by the Head of Corporate Finance. The integrity group model used is the approach recommended by Police Scotland's Public Sector Anti-Corruption Unit and is already utilised in a number of Scottish local authorities. The Corporate Integrity Group's remit includes:

- undertaking a fraud and corruption risk assessment and compiling an integrity risk register
- assisting with the development, review and communication of policies and procedures to mitigate the risk of fraud and corruption
- highlighting emerging risks, threats, vulnerabilities and related fraud and corruption opportunities
- receiving, considering and monitoring organisational vulnerability alerts / fraud and corruption flags and developing appropriate mechanisms for reporting and communicating these as appropriate
- agreeing appropriate actions to mitigate the fraud and corruption risks identified, including sustainable preventative measures
- raising awareness of fraud and corruption in the council as a method of prevention
- developing an action plan to implement / address the above and keep the response proportionate to the risks
- ensure proper communication and exchange of information with other groups e.g. Serious Organised Crime Group.

45. Police Scotland has also asked to work jointly with the council to pull together a case study on the fraud that would be valuable in getting the resilience message across Scotland's wider public sector. It is envisaged that this case study would also be used to inform various groups across the public sector including: the Local Government Directors of Finance (Scotland) Group and the Scottish Local Authorities Chief Internal Auditors Group.

Responsibilities for preventing and detecting fraud

46. Councils are responsible for developing and implementing effective systems of internal control as well as financial, operational and compliance controls. They are also responsible for establishing arrangements for the prevention and detection of fraud, error and irregularities, bribery and corruption and also to ensure that their affairs are managed in accordance with proper standards of conduct by putting proper arrangements in place.

47. The auditor is required to review those arrangements as part of their responsibility for assessing the suitability and effectiveness of the council's corporate governance arrangements, as required by the Code of Audit Practice. External auditor reports have not identified any weaknesses in the council's overall arrangements for the prevention and detection of fraud.

48. The previous external auditor reported in 2011/12, 2012/13 and 2013/14 that system reconciliations were an improvement area for management to address, although the issues raised were not specifically in relation to either the construction system or the fleet management system. Management agreed to document the key reconciliations that are undertaken around the various financial and non-financial systems operated by the council and to review the sufficiency of each reconciliation and implement an improvement action where required. The external auditor also reported in 2011/12 that the council did not undertake supplier statement reconciliations, with management agreeing that this would be implemented on a sample basis. The reports on the audits of 2014/15 and 2015/16 did not highlight any issues in relation to these areas.

49. As referred to at paragraph 1 above, the current external auditor, appointed in 2016/17, reported on the fraud in her latest annual audit report.

Audit Conclusions

50. Failures in fundamental controls within the council allowed this fraud to continue over a prolonged period. From the 57 fraudulent transactions only 2 were detected by the control systems in operation and resulted in the investigations.

51. On discovering the fraud appropriate action was taken by management as follows:

- individual - immediately suspended and access to systems removed. Disciplinary meeting held timeously where the employee resigned.
- investigations - the review undertaken were appropriately scoped to provide evidence of the fraudulent payments; identify the control weaknesses; and provide assurance that no further frauds had occurred.
- Police Scotland - informed timeously of the council's findings from the reviews and co-operated with the investigations. This resulted in the individual pleading guilty to the embezzlement of £1,065,085 from the council and he was sentenced to 5 years 4 months imprisonment.
- recovery of fraudulent payments - full recovery of the loss has been achieved with the exception of the £10,000 policy excess and £8,663 of PwC fees.
- control improvements - recommendations arising from the two PwC reviews have been implemented with the exception of system and process documentation which is nearing completion and is linked with the implementation of the new construction system which is planned to go live in August 2018. Follow-ups to the PwC reports are to be incorporated into internal audit's 2018/19 plan to provide assurance that the implemented controls are operating effectively.

52. The wider lesson from this incident, for other councils to consider, is the importance of key internal controls. These are documented in Appendix C and cover areas such as: segregation of duties (including user access rights); effective reconciliations; system documentation; and effective budget monitoring.

Appendix A - PwC recommendations

Ref.	Findings	Recommendations
1.	**Restricted access for privileged system users** The method used to process the fraudulent payments was the result of over-reliance on a single individual within IT who abused his privileged access rights. The user had access to systems right across the purchase to payable cycle and was able to use that access to execute the fraud.	Restricting system access rights, and, where possible, segregating responsibilities, limits the ability of any one user being able to bypass system enforced segregation of duties controls. An analysis should be undertaken across the council's financially significant systems, to identify all system administrators and super-users. Where conflicting access rights exist, these access rights should either be segregated or, if segregation is not possible, then monitoring of that user's access should be implemented. The next step is to undertake a wider review of system access for all users across financially significant systems, focusing on identifying potential segregation of duties conflicts and defining the access users require for their job role and responsibilities.
2.	**Interface reconciliations** It is our view that effective interface reconciliation controls may have helped identify the fraudulent transactions earlier.	Controls should be implemented to verify the completeness and accuracy of the data being interfaced between sub-systems and the general ledger. Any differences identified should be investigated and resolved.

Ref.	Findings	Recommendations
3.	**Balance sheet reconciliations** DCC did not conduct a balance sheet reconciliation from the Tranman subsystem to the general ledger. Such a reconciliation would have shown the fraudulent invoices 'routed' through this system. DCC did conduct a balance sheet reconciliation for the Construction subsystem but this was an ineffective control.	It is recommended that DCC reconsider the balance sheet reconciliations that they are performing to determine if there are any missing reconciliations (such as the Tranman reconciliation) and whether the reconciliations that are currently taking place are effective.
4.	**Supplier statement reconciliations** DCC did not conduct any supplier statement reconciliations on the supplier accounts that MC placed his false invoices into. While it is accepted that this may not be practicable for the construction subcontractors, a monthly supplier statement reconciliation of the Scottish Fuels account should have revealed the fraudulent invoices that were 'routed' through the Tranman sub-system.	It is accepted that conducting supplier statement reconciliations is resource intensive, but we recommend that DCC consider whether they could conduct reconciliations on key supplier accounts, where it would be easiest to 'hide' fraudulent invoices.
5.	**System limitations** It is clear that the limitations of the current construction sub-system, DCS, have had a pervasive impact across the control environment, undermining the effective operation of segregation of duties, interface, and balance sheet reconciliation controls. Management have identified that the system is no longer fit for purpose and the process is underway to procure a new construction sub-system to replace the existing construction sub-system.	Until a new construction sub-system can be procured and implemented, management will need to consider the practicalities of developing a short term fix to address these issues.

Ref.	Findings	Recommendations
6.	**System and process documentation** DCC do not have detailed system notes and mapping which articulate the flow of transactions and sets out how the interfaces work. This lack of documentation, while not a factor in enabling the fraud, was a contributing factor in the difficulty in tracking the accounting entries, as DCC could not demonstrate how the accounting systems actually worked. In order to gain an understanding of how the processes were working, PwC had to track entries through the systems, seeking to understand on a step by step basis what was happening at each stage of the process. This task, which was time consuming and labour intensive, would have been significantly streamlined had systems documentation been available. This lack of documentation places DCC at increased operational and financial risk should an unexpected event befall any of its IT systems in future.	DCC should document the processes and accounting pathways for each of its systems to ensure that they have a record of how these systems operate for future reference.

Source: PwC report Phase 1

.

Appendix B - Timeline

Date	Event
27 April 2016	Invoice added to system marked Prompt Payment.
20 May 2016	Finance doing year end work and noticed one payment had no invoice or remittance slip.
23 May 2016	On investigation data was going missing from live system, and call logged with IT.
24 May 2016	IT officer assigned call and spoke to finance staff, trace put on payment.
25 May 2016	IT officer advises payment was made into his bank account in error and this money would be refunded into the council's bank account.
26 May 2016	IT officer is suspended from duties and all access to buildings and computer systems is disabled.
30 May 2016	Police Scotland notified of the incident.
6 June 2016	PwC discussion around scope of work for Phase 1 review.
9 June 2016	A formal disciplinary meeting arranged – IT officer resigns from his post.
13 June 2016	Council Leader, Depute Leader and Group Secretary advised of incident.
14 June 2016	PwC begin working with the council.
July to Oct 2016	Chair of Scrutiny Committee and other senior politicians briefed on fraud and action being taken.
6 October 2016	Police Scotland advise officers of fraudulent payment pre 2012.
26 October 2016	PwC report to officers on fraud - Phase 1.
27 October 2016	Briefing with senior politicians from cross parties.
2 November 2016	Briefing for senior politicians and the Administration Group
19 December 2016	Agreed scope of work for Phase 2 of PwC investigation.
19 April 2017	Scrutiny Committee Members briefing on fraud.
1 June 2017	PwC report to officers on Phase 2.
2 August 2017	Individual pleads guilty to embezzling £1.065 million.
24 August 2017	Individual sentenced to 5 years 4 months imprisonment.
5 December 2017	Members briefing on fraud.
13 December 2017	Report to Scrutiny Committee on fraud

.

Appendix C - Lessons for other councils to consider

Whilst the fraud was complex, weaknesses in the council's key internal controls, facilitated the fraud and meant that it was not detected for some time. Other councils could learn lessons from this incident. They should consider whether the following fundamental internal controls are operating effectively:

- segregation of duties: ensuring access to systems are restricted to appropriate levels (to negate the possibility of individuals processing transactions all the way through the payments process).
- reconciliations: ensuring feeder systems are effectively reconciled to other systems (e.g. general ledger); using third party information (supplier's statements) and reconciling with payment systems.
- system documentation: system documentation should be maintained which details key controls to be carried out by staff to prevent fraud or error.
- budget monitoring: budget monitoring should be at a level that would allow budget holders to identify anomalous payments at an early stage.