

Stirling Council

Management Report 2017/18



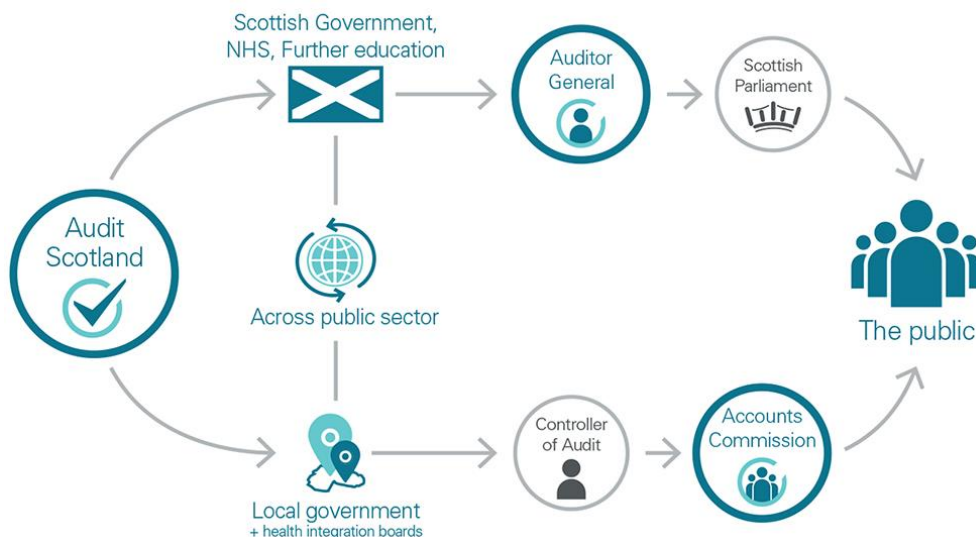
 **AUDIT SCOTLAND**

Prepared for Stirling Council
May 2018

Who we are

The Auditor General, the Accounts Commission and Audit Scotland work together to deliver public audit in Scotland:

- The Auditor General is an independent crown appointment, made on the recommendation of the Scottish Parliament, to audit the Scottish Government, NHS and other bodies and report to Parliament on their financial health and performance.
- The Accounts Commission is an independent public body appointed by Scottish ministers to hold local government to account. The Controller of Audit is an independent post established by statute, with powers to report directly to the Commission on the audit of local government.
- Audit Scotland is governed by a board, consisting of the Auditor General, the chair of the Accounts Commission, a non – executive board chair, and two non – executive members appointed by the Scottish Commission for Public Audit, a commission of the Scottish Parliament.



About us

Our vision is to be a world – class audit organisation that improves the use of public money.

Through our work for the Auditor General and the Accounts Commission, we provide independent assurance to the people of Scotland that public money is spent properly and provides value. We aim to achieve this by:

- carrying out relevant and timely audits of the way the public sector manages and spends money
- reporting our findings and conclusions in public
- identifying risks, making clear and relevant recommendations.

Contents

Audit findings	4
Introduction	4
Conclusion	4
Work summary	4
Risks identified	5

Audit findings

Introduction

1. This report contains a summary of the key issues identified during the interim audit work carried out at Stirling Council. This work included testing of key controls within financial systems to gain assurance over the processes and systems used in preparing the annual accounts. We will consider the results of this testing when determining our approach to the audit of the 2017/18 annual accounts.
2. Our responsibilities under the [Code of Audit Practice](#) require us to assess the system of internal control put in place by management. We seek to gain assurance that the council:
 - has systems of recording and processing transactions which provide a sound basis for the preparation of the financial statements
 - has systems of internal control which provide an adequate means of preventing and detecting error, fraud or corruption
 - complies with established policies, procedures, laws and regulations.
3. Also, we carried out work on the audit dimensions as required by the [Code of Audit Practice](#). This focussed on financial management, financial sustainability, governance and transparency and value for money.

Conclusion

4. We did not identify any issues which present a risk of material misstatement for the 2017/18 financial statements. However, we have reported in [Exhibit 1](#) a number of other issues and risks to management for consideration. We do not consider that any additional audit testing is required as a result of these issues. Overall, the operation of the key controls in place for each accounting system tested by us is considered to be satisfactory.

Work summary

5. Our 2017/18 testing covered key controls in a number of areas including bank reconciliations, payroll validation and exception reporting, authorisation of journals, change of supplier bank details and IT access controls. Additionally, we tested controls in the following areas: budget monitoring and control; feeder system reconciliations and controls for preventing and detecting fraud in areas such as taxation receipts, welfare benefits, grants and other claims. We also assessed the financial controls within the Swift social care payment system to support the assurances required for the audit of the Clackmannanshire & Stirling Integration Joint Board.



Bank reconciliations



Payroll controls



IT access



Budgets

6. In accordance with *ISA 330: the auditor's response to assessed risk*, our audit judgements are based on current year testing of controls and where appropriate prior year results. Our risk based audit approach allows us to take a three-year cyclical approach to controls testing. This approach enables us to place reliance on previous years' audit work where controls remain unchanged and no significant weaknesses had been identified. Also, where possible we place reliance on the work of internal audit to avoid duplication of effort.
7. The contents of this report have been discussed with relevant officers to confirm factual accuracy. The co-operation and assistance we received during the course of our audit is gratefully acknowledged.

Risks identified

8. Whilst no errors have been identified as a result of our audit work to date, the key control weaknesses identified during the interim audit are set out in [Exhibit 1](#). These findings will inform our approach to the financial statements audit, including any necessary additional substantive testing where relevant.
9. Any weaknesses identified represent those that have come to our attention during the course of normal audit work and therefore are not necessarily all the weaknesses that may exist. It is the responsibility of management to decide on the extent of the internal control system appropriate to Stirling Council.

Exhibit 1

Key findings and action plan 2017/18

Issue identified	Management response	Responsible officer and target date
<p>Audit findings</p> <p>Self-authorisation of journals</p> <p>Our sample testing of journals identified that some can be raised, posted and authorised by a single officer. Although monthly monitoring of journals is carried out by Finance, there is limited evidence of this, or whether it extends to verifying individual journals processed. The council should consider implementing a more regular and evidence based review of journals on a sample basis to support the early detection of potential errors.</p> <p>There is a risk that invalid or erroneous journals are not identified, potentially causing a misstatement within the accounts.</p>	<p>A report will be produced on a monthly basis from the ledger system providing details of processed journals. The Senior Accountants will review the processed journals on a sample basis and sign the report to evidence that they have checked the validity of the journals.</p>	<p>Accounting Operations Manager June 2018</p>
<p>Payroll exception reporting</p> <p>A number of payroll reports are reviewed after each payrun to identify any unusual or potentially erroneous entries. This is done on an informal basis, therefore there is limited</p>	<p>Since the audit the payroll section has introduced a spreadsheet documenting the various checking reports and tasks that are undertaken as part of the checking, and these are marked to</p>	<p>Payroll Manager Implemented May 2018</p>

Issue identified	Management response	Responsible officer and target date
<p>evidence of an audit trail for the work completed. The payroll reports are not signed off as reviewed and there is no evidence to demonstrate whether action has been taken to address issues identified within the reports. The council should consider implementing a more formal process for the review and follow up of payroll exception reports.</p> <p>There is a risk that unusual transactions are not identified and investigated resulting in errors in the accounts.</p>	<p>evidence that these checks have taken place for each payrun.</p>	
<p>Payroll access rights</p> <p>The council have recently implemented a combined HR/Payroll system. Our sample testing of user access rights identified that some employees have access to both the HR and Payroll sides of the system. Our sample included 3 users with 'HR Administrator' access as well as 'Payroll Generic' permissions. It is therefore feasible that these users could set up a new employee on the system and then also set up bank details in order for them to be paid. The council should ensure that there is appropriate segregation of duties when granting system access rights for those users who require access to both sides of the system.</p> <p>There is a risk that users with access to both sides of the HR/Payroll system could create a false employee. This may result in fraudulent payments being made.</p>	<p>The Council has operated a combined HR & Payroll Team since 2008. As we all work together in the same office and due to the number of team members it is not practical to maintain the same segregation that we did in previous years when the HR Team was spread across various parts of the Council.</p> <p>The previous HR & Payroll system was always a combined system and the new iTrent system is configured in such a way that there are even more overlaps, so in system terms there aren't two sides.</p> <p>We have carefully considered the access available through each User Access type and consider it to be appropriate.</p> <p>The Payroll Manager considers that there is sufficient segregation to allow the service to operate efficiently and have sufficient control over the data through the numerous checks carried out as part of daily processing.</p>	<p>Payroll Manager Risk accepted</p>
<p>Reconciliations not completed timeously</p> <p>Our audit testing established that the reconciliation between the sundry debtor account balance on the ledger and the cash receipting system for November 2017 was not completed until late January 2018. Furthermore, the reconciliation of payments received through the Orbis NDR system to the cashbook for September and October 2017 were not completed until January 2018. This was due to dependence on a key officer who was absent through illness and indicates that other members of the team do not have the</p>	<p>It is recognised that delays in both reconciliation processes were due to staff sickness.</p> <p>In terms of the sundry debtor reconciliation, another member of the Accounts team has the knowledge to carry this out.</p> <p>In terms of the NDR reconciliation, it is acknowledged that only one member of the Accounts team currently has the required skills to carry this out. As such, actions will be put in place to train an additional member of staff to carry out this task.</p>	<p>Accounting Officer June 2018</p>

Issue identified	Management response	Responsible officer and target date
<p>time, skills, or and knowledge required to undertake these tasks.</p> <p>There is a risk that financial discrepancies are not identified and resolved timeously.</p>		
<p>Non-Domestic Rates relief checks</p> <p>Relief awards should be reviewed periodically in accordance with the rates team's relief review timetable of reviewing all categories of reliefs every three years on a cyclical basis. Our sample testing identified one sports club relief claim which was last subject to review in January 2014. The next review of this category of relief is not due until June 2018. We reported a similar point in last year's interim management report. The council should monitor the review timetable to ensure that all required claim forms have been submitted by the appropriate deadline.</p> <p>There is a risk that discounts and reliefs are being awarded to those who do not meet the requirements.</p>	<p>Due to staffing issues during financial year 2017/18 we were unable to carry out the review of sports club reliefs.</p> <p>This will be carried out as a priority during June 2018.</p>	<p>Supervisor Payments</p> <p>June 2018</p>
<p>Authorisation of Swift social care payments</p> <p>Payments made by the council to care homes using the Swift system should be subject to review and countersigning by an appropriate officer. This control was in place and operating effectively up until staffing changes within the Business & Finance Team in September 2017. Since then, payments made to care homes have not been subject to a review/authorisation by a second officer prior to processing.</p> <p>There is a risk that inaccurate payments are being made to care homes through the Swift system.</p>	<p>Procedures will be put in place to reinstate the review and countersigning process by an appropriate officer.</p>	<p>Acting Team Leader, Business & Finance</p> <p>June 2018</p>
<p>Swift user access requests</p> <p>To ensure access to the system is appropriately restricted, the Business Information & Systems team issue request forms to those users requiring access. Upon their return, the authoriser of these forms should be checked against the authorised signatories list. Sample testing identified a user access request form signed by an officer who was not on the list. The user was therefore</p>	<p>A full review of SWIFT users and permissions was completed during 2017/18 and the authorised signatory list has also been updated.</p> <p>A rolling-review of SWIFT users and permissions including the authorised signatory list will be established so that records are continuously updated.</p> <p>A review of the SWIFT user access process is also due to take place during 2018.</p>	<p>Business Information Team Leader</p> <p>July 2018</p>

Issue identified	Management response	Responsible officer and target date
<p>granted access without appropriate approval by an authorised signatory. The council should ensure that all user access request forms are checked to the authorised signatory list.</p> <p>There is a risk that fraudulent activity may occur if inappropriate access to the system is granted.</p>		
<p>Swift – validation of payments</p> <p>We reviewed the process in place to validate care home resident information and payments made to providers. The council's Business & Finance Team issue a pro-forma directly to care home providers, with a requirement for the provider to complete and return the form in advance of the required payment date, as per the council's payment period timetable. While the process is operating effectively, areas for improvement have been identified. At present, the council send pro-formas to care homes by post or by e-mail. As these pro-formas contain sensitive information, any loss could lead to a data protection or security breach. The council should consider using a more secure method of communication such as Egress.</p> <p>There is a risk of a data protection or security breach should sensitive information be lost or sent to the wrong address.</p>	<p>The use of Egress is currently being considered with the intention that it will be implemented in the coming months. It is expected that there will be a period of dual running before full implementation.</p>	<p>Acting Team Leader, Business & Finance</p> <p>June - December 2018</p>
<p>Audit dimensions - issues and risks</p>		
<p>NFI approach</p> <p>The council actively participate in the National Fraud Initiative (NFI) exercise, including the investigation of ReCheck matches. The current approach adopted involves investigation of all ReCheck matches as opposed to focusing on those considered high risk or of high value. Although we note that the council demonstrate its commitment to NFI through allocating an appropriate level of time and resources to it, the approach could be more efficient. This would allow more time to be spent on high risk and high value areas, and also allow a more comprehensive review across the various categories of matches.</p>	<p>The Counter Fraud Officer will work with the officer responsible for completion of these matches to identify priority items for review at the point of matches being received. This risk-based approach will take into account high value areas for fraud and error.</p>	<p>Counter Fraud Officer</p> <p>June 2018</p>

Issue identified	Management response	Responsible officer and target date
------------------	---------------------	-------------------------------------

There is a risk that high value or high risk frauds or errors may not be investigated timeously.

Source: Audit Scotland

- 10.** All our outputs and any matters of public interest will be published on our website: www.audit-scotland.gov.uk.

Stirling Council

Management Report 2017/18

If you require this publication in an alternative format and/or language, please contact us to discuss your needs: 0131 625 1500 or info@audit-scotland.gov.uk

For the latest news, reports and updates, follow us on:



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