ABERDEEN
CITY COUNCIL

Internal Audit Report

Finance

Cash Receipting System

Issued to:
Richard Ellis, Interim Director of Corporate Governance
Steven Whyte, Head of Finance
Simon Haston, Head of IT and Transformation
Carol Smith, Accounting Manager
KPMG LLP

Date of Issue: November 2016 **Report No. AC1711**

EXECUTIVE SUMMARY

The Cash Receipting System is the main means by which income is controlled and processed for all activities of the Council, including the major revenues systems such as Council Tax, Business Rates, Housing Rents, and Debtors Invoices. During 2015/16, net income of £675.8 million was processed through the system relating to some 960,000 transactions.

The objective of this audit was to consider whether appropriate control is being exercised over the system, including contingency planning and disaster recovery, and that interfaces to and from other systems are accurate and properly controlled.

In general, the Cash Receipting System controls were found to be robust, well managed and adhered to. Areas identified for improvement included system procurement, system access, and information security and data protection training.

1. INTRODUCTION

1.1 The Cash Receipting System is the main means by which income is controlled and processed for all activities of the Council, including the major revenues systems such as Council Tax, Business Rates, Housing Rents, and Debtors Invoices.

1.2 During 2015/16, net income of £675.8 million was processed through the system relating to some 960,000 transactions. For the current year to 31 August, £295.8 million was processed relating to approximately 415,000 transactions.

1.3 The objective of this audit was to consider whether appropriate control is being exercised over the system, including contingency planning and disaster recovery, and that interfaces to and from other systems are accurate and properly controlled. This involved interviewing staff in the Service and in ICT, and testing system access and security, system operation and maintenance, interfaces, regulatory compliance, business continuity and disaster recovery.

1.4 The factual accuracy of this report and action to be taken with regard to the recommendations made have been agreed with Carol Smith, Accounting Manager, Sandra Massey, IT Manager, and Simon Haston, Head of IT and Transformation.

2. FINDINGS AND RECOMMENDATIONS

2.1 Written Procedures

2.1.1 Comprehensive written procedures which are easily accessible by all members of staff can reduce the risk of errors and inconsistency. They are beneficial for the training of current and new employees and provide management with assurance of correct and consistent practices being followed, especially in the event of an experienced employee being absent or leaving.

2.1.2 There are written procedures in place covering user set-up and administration; system input by cashiers; and the reconciliation processes. Procedures were reviewed and found to be comprehensive and up to date.

2.2 System Procurement and Upgrades

2.2.1 The system in use is the Icon Cash Receipting system provided by Civica; this has been the case since 2009, when it was procured through a Framework Agreement after approval from the Resources Management Committee. The system is partially hosted by the provider which means that it is supported and maintained by provider rather than the Council and the risk of holding confidential data is, for the most part, outsourced to the provider.

2.2.2 Under the terms of the contract system support currently costs the Council approximately £102,000 annually. The contract was renewed in 2015 to run for 7 years, at an additional one-off cost of £267,005 for the licence and consultancy, after exemption was granted by the Chief Executive, Head of Finance, Head of Commercial and Procurement Services, and Head of Legal and Democratic Services from Standing Orders, and this was reported to the Finance Policy & Resources Committee, ensuring that Standing Orders on Procurement were complied with.

2.2.3 The Civica Icon Cash Receipting system was procured using the Crown Commercial Service (CCS) Framework Agreement (Local Authority Applications RM1059 – Lot 2 Payment Processing and Cash Receipting Systems). Under the CCS Framework Agreement a Council may call-off a contract by direct award or further competition. A decision was made to make a direct award to Civica UK Ltd. Where a decision is made to award a call-off via direct award, the Council should have an audit trail of the methodology used in determining the most economically advantageous supplier under the Framework. Whilst legal advice included in the report to the Finance, Policy and Resources committee on 23 April 2015 indicated that it was not clear that this existed, information provided during the course of this audit has clarified the process followed in order to mitigate against the risk of breaching legal obligations and the EU Treaty Principles of fairness, openness and non-discrimination.

Recommendation
Consideration should be given to plan future tenders in line with EU procurement laws to allow time to change suppliers if required in the interest of competition.

Service Response / Action
Agreed. Future procurements will be planned earlier in line with the contract register.

Implementation Date	Responsible Officer	Grading
In line with contract register	Procurement and Service teams	Significant within audited area

2.2.4 Upgrades are installed by Civica and tested by Council ICT staff for stability. The system administrator within the Finance team carries out transaction testing and notifies Civica of system issues; a log is maintained of these issues and their resolution. System issues and downtime are notified to users through an email distribution list by the system administrator.

2.3 System Access & Security

2.3.1 In order to be granted access to the cash receipting system an email naming the employee and specifying the access required must be sent by a line manager to the Finance Systems Support team. Levels of access are available depending on role, ranging from view-only to system administrator. Once the user has been set up, the system administrator contacts ICT to request that user access to the system be permitted through their virtual desktop (VDE).

2.3.2 A sample of 15 active users was selected to confirm the authorisation process. Requests for 5 were not available. In 2 cases this was because the applications had been made before the current system administrator took on this responsibility and they had not been kept. In 3 cases this was because the users had been granted "Card Not Present – Supervisor" access only in order to check and report on online payments made to their Services, which does not permit payments to be taken by the user. Since the access was limited, the system administrator granted it without requiring authorisation.

2.3.3 Of the remaining 10, all were supported by emails from appropriate line managers. However, the information submitted in the emails was inconsistent. In 3 cases no information was provided on the new user's role in order to allow the appropriate level of access to be set. In another case, the email request implied that the user would only require access for two weeks in July 2016. However the access was still live at the time of testing in September 2016.

2.3.4 If access is granted inconsistently, or without proper authorisation, it is possible that incorrect levels of access could be granted. Failing to provide sufficient information in the initial request requires the system administrator to make follow up enquiries, which is an inefficient use of Council time and resources.

Recommendation
The Service should consider introducing a system access request form or template email in order to ensure all relevant information is provided to system administrators when creating user accounts.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
February 2017	Finance Controls Manager	Important within audited area

2.3.5 All users have unique IDs and their passwords comply with ICT guidance on security. An account will be locked if 3 incorrect password attempts are made, and can only be unlocked by the system administrator. If, when logged on to the system, a user is inactive for over 20 minutes, they will be logged off automatically.

2.3.6 Line managers are required to inform the Systems Support team when a staff member with Icon access leaves their position so that their access can be quickly disabled. Access is automatically disabled if the user does not log in for 90 days and can only be restored

on application to the Systems Support team. At present user audits are not carried out to confirm only active users in appropriate roles have access.

2.3.7 The accounts of 15 members of staff with access to the system who had left the Council were reviewed. 11 had been disabled automatically by the system after 90 days of inactivity while 4 were still active. The Service was notified and took action to inactivate these accounts.

2.3.8 If user accounts are not terminated promptly there is a risk that the system may be accessed inappropriately. While staff who have left the Council should no longer have access to the VDE, preventing access, staff moving to another role may retain their log-in. The Service advised that it was common not to receive leaver information from other Services but that a reminder would be sent to team leaders to ensure that this is corrected in future.

2.4 PCI DSS Compliance

2.4.1 PCI DSS (Payment Card Industry Data Security Standards) is a worldwide standard that was set up by the payment card industry to agree on minimum levels of security when processing and holding cardholder data. Compliance with the twelve PCI DSS requirements reduces the risk of fraudulent transactions and helps to shift liability for fraud from the merchant to the card issuer. The requirements cover all aspects of card payment transactions including software applications, telephony and communications networks, data storage and business processes.

2.4.2 As a 'merchant' processing transactions, Aberdeen City Council requires a 'payment services provider' (Civica) to capture payment card details and an 'acquirer' (WorldPay Streamline) to securely authenticate transactions and process payments to the Council's bank account. Acquirers may be fined by card issuing schemes such as Visa and MasterCard if their merchant customers are not compliant with PCI DSS requirements and there is a data breach or evidence of fraud. Acquirers will therefore refuse service to merchants who do not show evidence of compliance. This loss of service would mean that the Council would no longer be able to take payments by card. The Council may also be liable to a fine from the Information Commissioners Office in the event of a loss of personal information, and would risk reputational damage.

2.4.3 The acquirer, being liable for financial losses in cases of non-compliance, requires their customers to regularly complete a Compliance Self Assessment Questionnaire (SAQ). In addition, merchant compliance with PCI DSS requires that third party providers must also demonstrate compliance. Civica Icon has Level 1 PCI DSS accreditation and has provided a PCI DSS Compliance Statement to the Service.

2.4.4 Of the twelve PCI DSS Requirements, eight relate to network and computer system security and monitoring. The Service works with ICT and Civica to ensure that these requirements are met. A further three require that strong access control measures be in place, with access to systems which process cardholder data restricted to users with a business need for access. These users must be authenticated and identifiable and physical access to cardholder data should be restricted.

2.4.5 The twelfth requirement is the maintenance of an information security policy. The Council has an Information Security Policy and a Data Protection Policy, and requires all employees who use computers to complete Data Protection Essentials and Information Security Training. Of the 5 members of the Income Support team, 1 had not completed either course at the time of audit, while a further 2 had not completed Data Protection training. The risks of failing to fully train staff in information security are outlined in 2.4.2

above. The Service advised that the team manager was in the process of ensuring that all staff had completed the training; a recommendation is included to track progress.

Recommendation
The Service should ensure that all appropriate staff complete For Your Eyes Only and Data Protection Essentials training.

Service Response / Action
Agreed.

Implementation Date	Responsible Officer	Grading
April 2017	Finance Controls Manager	Significant within audited area

2.5 Interfaces

2.5.1 The cash receipting system interfaces with eFinancials (debtors system); iWorld (Housing); Academy (Council Tax); Northgate (Business Rates); Accord Card (school meals and other general payments); the parking payments system; the planning system; and ELMS Portal (licensing system).

2.5.2 Interface files run overnight, following a schedule, and are monitored by Systems Analysts in ICT. The system has a number of automated checks which identify failures and send emails confirming success or notifying failure to the Systems Analysts, who take appropriate action.

2.5.3 Copies of the emails retained by the Systems Analysts were obtained and reviewed. There have been two instances in the current financial year where part of the interface failed. In both instances the cause of the failure was identified within a day and a fix was applied.

2.6 Reporting & Reconciliations

2.6.1 The Income Support Officer runs a daily search through the financial data systems specialist Transaction Network Services International (TNS) portal to identify failed card payment transactions and those which were successful but were not transferred to the Icon system. The results are input to a card income reconciliation spreadsheet and matched against Icon figures. Any variances are investigated and corrected by the Income Support team where possible. On occasion technical issues mean successful payments are not automatically recorded in Icon and need to be transferred manually by Civica. The card income reconciliation spreadsheet was reviewed and found to be operating effectively.

2.6.2 The Income Support Officer is responsible for reconciling the cash receipting system to other feeder systems and the ledger. These reconciliations are carried out daily as part of the Bank Reconciliation procedures, which were reviewed in audit report AC1616.

2.6.3 The cash receipting system is reconciled to the Ledger. Fund analysis reports are run and these are compared to postings in the Ledger. All variances are investigated and resolved.

2.6.4 The reports were re-run by Internal Audit for each day of the week of 4 - 8 July and they included all relevant accounts and Funds. The values were matched to the reconciliation spreadsheet and the calculations were confirmed correct. On one day (5 July) the original totals did not match as the Ledger was £147 short; this payment was tracked down by the

Income Support team as a transaction credited on 5 July in Icon but not in the ledger until 6 July. This was included in the spreadsheet as a correction and the totals then reconciled.

2.6.5 System reconciliations are also carried out by the Income Support Officer between the cash receipting system, the ledger, and figures from system reports for Housing Benefit overpayments and Council Tax (Academy), Housing Rents (iWorld), Business Rates and Business Improvement District (BID) transactions. A three way match is required, with the exception of Rents, which are not currently compared to the ledger (considered in audit AC1607 Rent Collection (2.2.4)). The results of these reconciliations are reported to the relevant Service Accountants.

2.6.6 All system reconciliation spreadsheets were observed to contain daily entries, all of which had been input timeously and investigated where necessary. All spreadsheets were observed to be operating effectively, with one exception. In the Council Tax reconciliation sheet, in two cases the totals from the system report did not match those entered into the Daily Balance sheet, as Universal Credit debits had not been included in the calculation. This was because the relevant column in the Daily Balance sheet had been linked incorrectly and was picking up data from the Suspense Account column in the System sheet, rather than from the 'U/C' column as required. The Service advised that the reconciliation spreadsheet has now been amended and the sheets are now linked correctly.

2.7 Business Continuity & Disaster Recovery

2.7.1 An "Incident response plan" is required under PCI DSS 12.10. The Icon system is included in the most recent version of the Finance Service Business Continuity Plan which was updated in August 2015. Data is backed up on a nightly basis by Council database administrators. Data restoration is tested twice a year.

2.7.2 Disaster Recovery (DR) within the Council is the shared responsibility of the Emergency Planning team and the Data Centre service provider. After transfer to a new Data Centre provider (Brightsolid) in the first half of 2016 temporary measures are in place until DR exercises can be carried out. The ICON system is considered critical and is included in DR planning.

AUDITORS: D Hughes
A Johnston
L Jarvis

Appendix 1 – Grading of Recommendations

GRADE	DEFINITION
Major at a Corporate Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss, or loss of reputation, to the Council.
Major at a Service Level	The absence of, or failure to comply with, an appropriate internal control which could result in, for example, a material financial loss to the Service/area audited. Financial Regulations have been consistently breached.
Significant within audited area	Addressing this issue will enhance internal controls. An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on a system's adequacy and effectiveness. Financial Regulations have been breached.
Important within audited area	Although the element of internal control is satisfactory, a control weakness was identified, the existence of the weakness, taken independently or with other findings does not impair the overall system of internal control.