Ordering and Creditor Payments 2016-17

City of York Council

Internal Audit Report

Business Unit: Customer and Corporate Services Directorate
Responsible Officer: Director of Customer and Corporate Services
Service Manager: Head of Business Support
Date Issued: 30.01.18
Status: Final
Reference: 10180/008

	P1	P2	P3
Actions	**0**	**1**	**2**
Overall Audit Opinion	Substantial Assurance		

Summary and Overall Conclusions

Introduction

Ordering and creditor payment systems are audited regularly because of their importance to the council's operations, the value of transactions and the potential for fraud. Creditor payments is a key service within the council, processing over £200m worth of payments and nearly 50,000 invoices between September 2015 and October 2016.

Completion of purchase orders is a key part of the council's financial regulations and since December 2012 the council has had a 'no purchase order, no payment' policy. Purchase orders are vital in controlling council expenditure, achieving best value and realising efficiencies in the 'purchase to pay' system.

The creditor payments service is also responsible for ensuring that invoices are appropriately authorised before payment and that they are paid promptly according to council targets and supplier requirements.

Objectives and Scope of the Audit

The purpose of this audit was to provide assurance to management that procedures and controls within the system will ensure that:

- ordering and creditor procedures comply with the council's financial regulations, relevant legislation and best practice;
- the ordering process is robust and the official system is used for purchasing goods and recording when these have been received;
- payment systems are secure, payments are only made for valid invoices and for the correct amount;
- invoice processing systems are efficient and timely and there are appropriate performance management arrangements in place;
- non-standard (i.e. without an order or invoice) creditor transactions are correctly accounted for by the creditors system and related accounting records.

Key Findings

The proportion of invoices with accompanying purchase orders (CRIPO), against sundry invoices (CRINV) remains high at 84% and deliberate changes to creditor processes for manual payments would need to be made to increase performance. The scheme of delegation has been reviewed as part of a new annual exercise and new authorisation levels have been set for every user profile on the purchasing system. It is intended that a review of the scheme of delegation will be undertaken every year to ensure that authorisation levels are appropriate and the next Ordering and Creditor Payments audit will observe whether this is taking place.

There is an appropriate segregation of duties in the requisitioning, authorising and goods receipting processes of CRIPO payments and orders are approved within delegated authority limits. Goods/services ordered via the official purchasing system are receipted on delivery and the invoices sampled agreed to the items ordered on the purchasing system. CRINV invoices (invoices without corresponding POs) are approved for payment by managers with the appropriate delegated authority. Pro formas are completed for payment requisitions (CRREQ) transactions and contain a separation of duties in the requisitioning and authorising process. CRREQ payments are also appropriately authorised before submission for payment.

CRINV/CRIPO and payment performance reports are still generated on a regular basis from the FMS system and emailed to relevant staff members. A performance dashboard has recently been developed which will allow the Finance team to monitor and respond to trends in the data. The next audit will observe how effectively this tool is used. Currently, approx. 90% of invoices are paid within the set target of 30 days from the recorded date of receipt of the invoice.

There is an acceptable segregation of duties in the payments run process, with control totals and potential duplicate payments checked by the Creditors team and BACS files processed by the IT Operations officer. In the majority of cases, requests for new supplier records are appropriately authorised by budget holders and the procurement team. In some cases documentation has not been retained, resulting in some records of authorisations being absent. It should be ensured that these records are retained.

The Creditors team maintain procedure notes for higher risk processes e.g. pay runs, authorisation of various types of payments, processing of file interfaces, etc. In the majority of cases they are up to date, though still quote the personal names of individuals that have left council employment. The council may wish to review and update these documents to ensure their relevancy. The number and age of items in the dispatcher at the time of audit testing indicates that payment officers attempt to resolve vouchers in dispute in a timely fashion. The voucher register is regularly checked and cleared to ensure that discrepancies are resolved.

Whilst sufficient controls are in operation in the majority of cases, there are a few issues which require attention from management and these are detailed below.

Access levels for Creditors staff require review and adjustment, to ensure that they do not have the permissions to both process and authorise invoice transactions in the FMS software. Evidence is not always available to show that there is an appropriate segregation of duties in the requisitioning process for manual payments (CRINM). Evidence is not always available that the Creditors team are performing the requisite identity checks on individuals requesting a change to creditor bank account details.

Overall Conclusions

The arrangements for managing risk were good with few weaknesses identified. An effective control environment is in operation, but there is scope for further improvement in the areas identified. Our overall opinion of the controls within the system at the time of the audit was that they provided Substantial Assurance.

1 FMS software access levels

Issue/Control Weakness	Risk
FMS software access levels currently allow the Creditors team to both process and authorise CRINV (sundry invoice) and CRIPO (invoice with corresponding purchase order) transactions.	Transaction details may be inappropriately adjusted before they are submitted to the pay run, potentially resulting in payments of incorrect value or payments made to incorrect creditors.

Findings

When an invoice is received by the Creditors team, they validate, process and authorise the invoice on the FMS software before submission to the pay run. Whilst audit testing demonstrated that there is an appropriate segregation of duties in the requisitioning, authorising and goods receipting processes before the invoice is entered onto FMS, testing also identified that members of the Creditors team are capable of processing, amending and authorising invoice transactions on FMS. Instances of this occurring were not identified during audit testing, however, this is a fundamental segregation of duties which should be mandated by the system.

Access levels for Creditors staff require review and adjustment, to ensure that they do not have the permissions to both process and authorise CRINV and CRIPO transactions. This is particularly essential for CRIPOs, as they have the capability to adjust all transaction details before submitting them for payment.

Management Response

The separation of duties procedure ensures that the same person does not process and authorise a transaction and no instances of this ever occurring have been identified. The test system does not allow this to happen and whilst the audit identified it was technically possible within the live system, no payment was made. It is also important to note that Creditors are required to amend some transaction details in terms of correcting VAT codes and adjusting for minor variations but that there are strict procedures in place to ensure that whenever a member of staff needs to make an amendment, this is subsequently verified by another member of the team.

Agreed Action 1.1

The FMS access levels of the Creditors team will continue to be tested and adjusted as necessary to ensure that they can not both process and authorise CRINV (sundry invoice) and CRIPO (invoice with corresponding purchase order) transactions.

Priority	2
Responsible Officer	Business Support Manager - JK
Timescale	Jan 18

2 CRINM payments

Issue/Control Weakness	Risk
It is difficult to conclude whether there is an acceptable separation of duties in the authorisation process for CRINM (manual creditor) payments or whether they are always authorised within delegated limits.	There is an increased risk that inappropriate or inaccurate payments could be made.

Findings

Manual creditor payments are submitted to the Creditors team via a template pro forma with separate fields for the requesting and authorising officers. These payments total approx. £91 million in the audit period tested, mainly comprising of large value payments to other authorities and government bodies. It was not always possible to judge whether the sample of pro formas tested had been appropriately authorised, as they were only signed with two letter initials. These initials were not always legible. In a couple of cases, the 'authoriser' field was blank.

As CRINM transactions are almost exclusively routine payments made to other local authorities and government bodies, the risk of the payments being inaccurate or irretrievable is lower than those paid to suppliers or private individuals. Evidence of inappropriate payments was not identified during audit testing, however, the process for authorisation of CRINM payments requires review and the pro forma could potentially be adjusted to ensure that employees are required to clearly state their identity.

Management Response

These are almost exclusively routine payments made to other local authorities and government bodies, and therefore there is limited possibility of any inaccuracies. In the unlikely event of errors, the impact would be minor. In terms of both frequency and impact, there is a only very small risk. In addition, no evidence has been found during testing to suggest that any inappropriate payments have been made. In terms of both frequency and impact, there is a only very small risk.

Agreed Action 2.1

Pro formas for both CRINM (manual creditor) and CRREQ (requisition) payments will be reviewed and adjusted to ensure that requisitioners and authorisers must state their identity. Instructions on the intranet will also be adjusted to specify that the pro formas must be sent from the authoriser’s email address. A reminder will be issued to the scanning team to always scan both the batch processing form and the pro forma for each transaction.	**Priority**	3
	Responsible Officer	Business Support Manager - JK
	Timescale	Jan 18

3 Changes to bank supplier details

Issue/Control Weakness	Risk
Evidence is not always available to confirm that the Creditors team are undertaking the correct identity checks when they receive a request to change bank account details.	Successful bank mandate fraud resulting in financial loss to the council.

Findings

Bank mandate fraud can occur when an individual purporting to be a representative of an organisation's creditor contacts that organisation and requests that the bank account details on the creditor account are adjusted. Payments due to the legitimate creditor are then diverted to the fraudster's bank account. The council’s policy document states that the Creditors team must confirm the identity of the individual submitting the request by a.) checking that the request has been made via the creditor's contact details held on their FMS record and, b.) by asking the individual to quote the creditor's old bank account details. These details can also then be verified by comparison with the FMS record.

A sample of requests was reviewed to ascertain whether these verification steps are followed. In the vast majority of cases, evidence was available to confirm that the team requested the creditor's old bank account details. However, there was no confirmation that they had also ensured the request had been made via the contact details/creditor representatives held on record.

It should also be noted that there are more sophisticated forms of bank mandate fraud; involving an individual requesting that creditor contact details are adjusted first, then requesting that bank account details be adjusted at a later date. It is recommended that the procedure for changes to creditor contact details ensure that similar identity checks are undertaken before adjustments are made to the FMS record.

Management Response

All changes to supplier bank details are checked and verified, however, the Creditors team will be reminded to retain the relevant evidence.

Agreed Action 3.1

A reminder will be issued to the Creditors team asking that they attach evidence of the creditor verification they have undertaken to FMS when changes to bank details have been requested. The policy document for changes to supplier bank details will also be adjusted so that the same verification steps will be undertaken when changes are requested to supplier contact details.

Priority	3
Responsible Officer	Business Support Manager - JK
Timescale	Jan 18

Annex 1

Audit Opinions and Priorities for Actions

Audit Opinions	
Audit work is based on sampling transactions to test the operation of systems. It cannot guarantee the elimination of fraud or error. Our opinion is based on the risks we identify at the time of the audit. Our overall audit opinion is based on 5 grades of opinion, as set out below.	
Opinion	**Assessment of internal control**
High Assurance	Overall, very good management of risk. An effective control environment appears to be in operation.
Substantial Assurance	Overall, good management of risk with few weaknesses identified. An effective control environment is in operation but there is scope for further improvement in the areas identified.
Reasonable Assurance	Overall, satisfactory management of risk with a number of weaknesses identified. An acceptable control environment is in operation but there are a number of improvements that could be made.
Limited Assurance	Overall, poor management of risk with significant control weaknesses in key areas and major improvements required before an effective control environment will be in operation.
No Assurance	Overall, there is a fundamental failure in control and risks are not being effectively managed. A number of key areas require substantial improvement to protect the system from error and abuse.

Priorities for Actions	
Priority 1	A fundamental system weakness, which presents unacceptable risk to the system objectives and requires urgent attention by management.
Priority 2	A significant system weakness, whose impact or frequency presents risks to the system objectives, which needs to be addressed by management.
Priority 3	The system objectives are not exposed to significant risk, but the issue merits attention by management.

Where information resulting from audit work is made public or is provided to a third party by the client or by Veritau then this must be done on the understanding that any third party will rely on the information at its own risk. Veritau will not owe a duty of care or assume any responsibility towards anyone other than the client in relation to the information supplied. Equally, no third party may assert any rights or bring any claims against Veritau in connection with the information. Where information is provided to a named third party, the third party will keep the information confidential.