INTERNAL AUDIT REPORT

FROM:	Audit and Risk Manager	**SUBJECT:**	Payment of Creditors
TO:	Head of Finance	**DATE:**	31 March 2023
C.C.	Chief Executive Strategic Procurement and Creditors Manager Senior Finance Admin Officer Portfolio Holder (Cllr Hales)		

1 Introduction

1.1 In accordance with the Audit Plan for 2022/23, an examination of the above subject area has recently been completed by Ian Davy, Principal Internal Auditor, and this report presents the findings and conclusions for information and, where appropriate, action.

1.2 Wherever possible, findings have been discussed with the staff involved in the procedures examined and their views are incorporated, where appropriate, into the report. My thanks are extended to all concerned for the help and cooperation received during the audit.

2 Background

2.1 The system in place for processing creditor transactions, from the ordering of goods and services through to the payment of the receipted invoices has changed from TOTAL to Ci Anywhere, with the new system going live in November 2021.

2.2 Payment to commercial suppliers in the year to date total £54.1m, covering over 4,200 invoices.

3 Objectives of the Audit and Coverage of Risks

3.1 The management and financial controls in place have been assessed to provide assurance that the risks are being managed effectively. It should be noted that the risks stated in the report do not represent audit findings in themselves, but rather express the potential for a particular risk to occur. The findings detailed in each section following the stated risk confirm whether the risk is being controlled appropriately or whether there have been issues identified that need to be addressed.

3.2 In terms of scope, the audit covered the following risks:

1. Orders are placed for which the service has no budget.
2. Orders (requisitions) are inappropriately authorised.

3. Ineffective payment processes (e.g. failure of auto-matching, staff not submitting invoices for payment when received directly etc.) leading to payments not being made.
4. Incorrect payments are made (e.g. payments for the wrong amount / duplicate payments / goods not received etc.)
5. Discounts for prompt payment are not received / penalties for delayed payments are incurred.
6. Non-order payments are inappropriately made.
7. Credit notes are processed incorrectly (e.g. credit not taken, paid as an invoice etc.)
8. Creditors are misrepresented in Council's Statement of Accounts.
9. Lack of accountability.
10. Recovery action taken and / or loss of access to goods and services due to payments not being made in a timely manner.
11. Payments against valid creditor invoices are misappropriated.
12. Collusion with creditors leading to fraudulent invoices being submitted / directly submitting fraudulent invoices for payment.
13. Supplier data inappropriately amended.
14. Loss of IT / access to the Ci Anywhere finance management system.
15. Inappropriate access to Ci Anywhere.
16. Failure of BACS system leading to payments not being made to creditors.

3.3 These were identified during discussion between the Principal Internal Auditor and the Senior Finance Admin Officer. The 'incorrect payments made' and 'failure of the BACS system' risks are also reflected in the departmental risk register.

3.4 The work in this area underpins the internal Money strand of the Council's Business Strategy.

4 Findings

4.1 Recommendations from Previous Reports

4.1.1 This section is not applicable as there were no recommendations raised as part of the last audit of the subject, undertaken in December 2018.

4.2 Financial Risks

4.2.1 Risk: Orders are placed for which the service has no budget.

The latest Code of Financial Practice highlights that 'All expenditure and income should be coded to the correct allocation code. Budgets can only be vired to match the expenditure or income, again, subject to the rules of virement. Income/Expenditure should not be coded to where the Budget is, where this code is not consistent with the actual activity.'

It goes on to say that 'Budget Managers will have freedom to move budgets within individual services as described in this section. In managing budgets, the overall priority is to ensure that the overall net expenditure on a specific service is within the overall budget for that service. Managers must take appropriate actions to ensure that this is complied with. Accordingly, whilst there may be variances alongside individual component budgets, managers need to take a strategic view of their budgets. This will entail them proactively viring between individual budget lines within a service budget. An overspend on one budget head should be compensated by an underspend on another.'

As such, there is no direct need to ensure that individual budget codes ('subjective' lines) are not overspent, as long as the individual budget for a service is controlled.

The Strategic Procurement and Creditors Manager (SPCM) highlighted that, within Ci Anywhere, individuals are defaulted to a delivery point (cost centre and activity code) with a search function allowing users with multiple codes to select the appropriate delivery point. In addition, the nominal element of a budget code is pre-set for all items included in the internal catalogue.

Whilst the nominal (and, therefore, the budget line) can be overwritten, this has not been publicised to users and the action is discouraged. The SPCM highlighted that the only area where the risk of selecting the wrong nominal remains is in relation to the use of capital monies through the project ledger as the coding has to be manually entered in this ledger.

Whilst individual budget codes can be overspent, there is control within the system to stop further orders being placed against contracts once the contract limit has been reached. This is dependent on there being a specific contract value being set within the system and the relevant box being ticked in the contract settings.

4.2.2 Risk: Orders (requisitions) are inappropriately authorised.

Sample testing was undertaken to ensure that the authorising officer for each requisition was appropriate (generally within the same service area) and that there was segregation of duties (i.e. the person who authorised the requisition had not also raised it). This testing revealed no issues.

4.2.3 Risk: Ineffective payment processes (e.g. failure of auto-matching, staff not submitting invoices for payment when received directly etc.) leading to payments not being made.

The Senior Finance Admin Officer (SFAO) advised that the auto-matching functionality is not working on Ci Anywhere (awaiting a system update), so all invoices are being manually matched to the orders. This will generally be against the order number quoted on the invoice although it may be amended if staff in the service area contact the Purchasing and Procurement Team (formerly the FS Team) to advise of changes.

The SPCM highlighted that the restructuring of the FS Team was in anticipation that this auto-matching functionality would be operational and, as a result, there remains a risk due to the manual nature of the process and the reduced resources available.

Testing undertaken confirmed that eighteen of the twenty orders sampled were matched to the order number stated on the invoice. In the other two cases, one was matched to a different order than that stated and one invoice did not include an order number. However, given the 'manual' matching process, it was confirmed that both invoices had been paid against the correct order on the system.

Guidance on the creditor invoice process, including the need to forward them to the relevant email address (invoices@warwickdc.gov.uk) is included on the Finance pages of the intranet, so all staff should be aware of the correct process to follow.

4.2.4 **Risk: Incorrect payments are made (e.g. payments for the wrong amount / duplicate payments / goods not received etc.)**

The sample selected for the test set out at 4.2.3 above was also reviewed to ensure that the invoices were appropriately detailed (i.e. they set out the goods / services provided, were addressed to the Council, and included their VAT registration number where appropriate) and had been correctly calculated, with the payments only being made once the goods had been receipted on the system. This testing proved satisfactory.

The results of the latest NFI exercise were examined (reports 707 – Duplicate Records by reference, amount, and creditor reference (values over £500) and 708 – Duplicate Records by amount and creditor reference (values over £1,000) to ascertain whether any duplicate payments had been made. These tests highlighted two duplicate payments totalling £17,140.

They were not picked up by the (Ci Anywhere) system controls as the invoice reference had been entered differently in one case and the other duplicate was due to a quote document being used for a payment and then the invoice was received and was also paid. The current lack of auto-matching on the system, as highlighted above, was considered by the SPCM to be a contributing factor to these errors.

The duplicate payments were flagged up with the relevant staff members and attempts were being instigated to get the funds returned.

4.2.5 **Risk: Discounts for prompt payment are not received / penalties for delayed payments are incurred.**

An intranet message is prepared on an annual basis advising staff that the Council has to publish an annual Payment Performance Data Report. As part of this notification, staff are reminded that the Purchasing and Payment Team are reliant on staff to notify them of any late payment fees that they are aware of.

Payment Performance reports were found to be up to date on the Council's website, covering the financial years from 2015/16 to 2021/22.

The SFAO advised that there is no requirement to provide an explanation of why the fees have been incurred or to provide details of any missed discounts (although suggested that the Council very rarely receives any 'offers' of prompt payment discounts)

Advisory

Staff should be asked to provide explanations for any late payment surcharges incurred.

The sample used for the tests above was checked to ensure that the payments were being made on a timely basis (i.e. on the next payment run after the receipt of the invoice / completion of the ordering and receipting process).

With two payment runs per week (Mondays and Wednesdays), the longest assumed gap for 'prompt payments) was considered to be five days (i.e. the process completed on a Wednesday after the payment run had been completed before the next payment run was undertaken on the Monday).

Whilst there were some large gaps between the invoice dates and the payment dates, the largest gap between the process being completed on the system and the payment being made was six days. In this instance there was no payment run on the Monday due to a bank holiday, so the payment had been made on the next run undertaken as appropriate.

One issue was however noted in that, in twelve of the twenty cases, the orders were actually raised on or after the date of the invoice.

Recommendation

Staff should be reminded of the need to raise requisitions in a timely manner.

If the ordering and goods receipting process has not been undertaken when the invoice is received or if there is a variance between the order and the invoice, the invoice will be 'suspended'. At the time of the audit testing, there were 54 suspended invoices, with half of these relating to Comensura (agency staffing).

The SFAO advised that when the invoice is suspended an email notification will be sent to the relevant staff member. On day seven (based on the creation date on the system), if action has not been undertaken to resolve the issue, the system escalates the case and an email will be sent to the Purchasing and Payment Team who will chase the department. A further alert will be sent on day 14 and then, on day 21, a further alert will be sent and the invoice will be deleted.

For Comensura invoices, the chasing is undertaken at day 21 and they are not deleted from the system with the invoices being balanced at year end.

The SFAO advised that it is not possible to note the chasing performed directly on the system so relies on emails being retained although some of the chasing is performed via phone calls, so there is not always evidence.

A sample of suspended invoices that had reached the different thresholds was reviewed and the SFAO was able to provide evidence of the chasing performed and sample system alerts in most cases and was able to explain what had been undertaken in the other cases.

4.2.6 **Risk: Non-order payments are inappropriately made.**

For some payments made, there is no requirement to raise an order on the system due to them being classified as non-commercial payments. Non-commercial payments arise due to the initial processes being undertaken on another system, or the payments being made are in respect of contributions, grants, refunds or any other payment that does not relate to the payment for goods, works or services.

Payments in respect of housing benefit, council tax and NNDR refunds are dealt with through CIVICA and those in relation to housing and other Council property assets having works orders placed on Active H. The SPCM advised that a project is in place to integrate Active H with Ci Anywhere so that commercial payments are correctly recorded within the system for spend and contract analysis and oversight.

For CIVICA, the (Exchequer) Systems Officer (ESO) will email the Purchasing and Payment Team with details of the transactions (number and amounts) and a file will be uploaded to the server. This is automatically picked up by Ci Anywhere which will create or overwrite accounts for each payment due, setting up non-order transactions and posting the transactions as ready for payment.

An alert is then generated which highlights that the transactions are ready for payment with the alert also detailing the number of payments and the amount.

A checklist is used to ensure that each of the payment runs is undertaken appropriately with the figures being matched. Once run, an email alert is sent to the ESO to confirm that the payments have been made.

As the process is automated, the last CIVICA payment run was reviewed which confirmed that the process had operated as expected.

For Active H, when Assets staff post a file, it automatically exports to a server file and they will email the Purchasing and Payment Team with copies of the invoices to support the payments.

Ci Anywhere picks this server file and uploads to a suspended non-order payment with an alert being sent to the Purchasing and Payment Team.

The Purchasing and Payment Team then update the relevant transaction and, when everything matches, the transaction is posted for payment and will be included in the next Commercial payment run.

There is a Commercial Run checklist, with the total amounts being checked, although this covers all relevant payments that have been included as opposed to anything specific for Active H. The SPCM advised that the route used for these payments may change as part of the integration mentioned above and the need for spend to be tracked in the purchasing and contracts module.

A sample of ‘other’ non-order payments was selected and testing was undertaken to ensure that appropriate supporting documentation has been uploaded to the system, with details of the correct supplier, amount, and reason for the payment. This test proved satisfactory with appropriate supporting documentation being in place for each payment reviewed.

4.2.7 **Risk: Credit notes are processed incorrectly (e.g. credit not taken, paid as an invoice etc.)**

A sample of credit notes received was reviewed to ensure that they were being used to offset the original invoice or were being claimed against a subsequent invoice from the supplier and they were being taken as credits (i.e. payment was not being made against the credit note received). No issues were identified.

4.3 Legal and Regulatory Risks

4.3.1 **Risk: Creditors are misrepresented in Council's Statement of Accounts.**

As highlighted above, the SFAO advised that all invoices are currently being matched to the orders raised, so there were no issues with regards to orders being shown as outstanding where a payment had already been made.

He also highlighted that all relevant Finance management staff and accountants have access to all relevant modules and dashboards that can be reviewed to look at the budget position and any commitments (i.e. orders placed that have not yet been paid).

4.4 Reputational Risks

4.4.1 **Risk: Lack of accountability.**

The current Code of Financial Practice includes sections on Expenditure and Payment of Accounts as well as making reference to the responsibilities in this area for the different levels of staff.

The Principal Accountant – Systems (PAS) is the system owner for Ci Anywhere although the Purchasing and Payments team, managed by the SFAO, has day to day ‘responsibility’ for the payment processing. This responsibility is reflected in the latest job description for the SFAO as appropriate.

The SFAO advised that there are no restrictions over which codes individual users can use when setting up requisitions. This is partly due to the fact that certain users (e.g. CST staff) will need to raise orders on behalf of various cost centres.

As highlighted above, codes will be auto-filled when requisitions are created from the contracts / catalogue of products on the system which will generally be relevant to the specific user although the codes can be amended or split if required.

The new user request form also requires the department cost code and activity codes to be provided, with the form highlighting that this will be the default code used when orders are raised.

There are four requisition approval limits set in Ci Anywhere (£10k, £50k, £200k and Unlimited), with three different 'role' types (Finance, Procurement and Standard).

The PAS advised that a decision had been taken to rationalise the number of different levels available, as TOTAL had become unwieldy to manage, with these four 'values' being considered to be sensible amounts.

Those who had approval levels on TOTAL were placed into the nearest equivalent level on Ci Anywhere, with new users having their level decided by their manager when they complete the new user request form.

4.4.2 **Risk: Recovery action taken and / or loss of access to goods and services due to payments not being made in a timely manner.**

Testing on the timeliness of payments is covered above (see 4.2.5).

4.5 Fraud Risks

4.5.1 **Risk: Payments against valid creditor invoices are misappropriated.**

The sample used for the previous tests was reviewed to ensure that the payments were being made to the correct bank account.

In two of the twenty cases, the payment was made to a different bank account than the one identified on the invoice but was in line with what was included on the standing creditor data at the time of the payment. The standing data had subsequently been amended in one case, but the other still showed the old bank account details.

Recommendation

Staff should be reminded of the need to check bank account details recorded on the invoice against the standing data before a payment is made.

4.5.2 **Risk: Collusion with creditors leading to fraudulent invoices being submitted / directly submitting fraudulent invoices for payment.**

As highlighted in the findings above, all invoices paid had been matched to appropriately authorised orders.

Within the permission settings for each role, there is a 'tick box' that either allows or does not allow a user to approve their own purchase requisitions. The PAS attempted to raise and authorise a requisition during the audit testing and an error message was received as expected.

An extract was run from Ci Anywhere showing all requisitions. Upon review of the completed requisitions, the only ones shown as being created and approved by the same user were those that had been created by an admin user when they were imported onto Ci Anywhere from TOTAL.

As highlighted at 4.2.2 above, the testing of requisition approvals also looked at the segregation of duties for these requisitions with no issues identified.

4.5.3 Risk: Supplier data inappropriately amended.

Similar to the above, the ability to modify creditor standing data (accounts payable account (details) and accounts payable bank account) is set within the permissions for each role.

Those with Finance permissions can change the standing data, although the SFAO advised that they would still generally complete a form to get the changes approved.

The creditor account screens on Ci Anywhere include 'audit details' that show when the account was last amended and the user that undertook the change. By clicking through to the audit details, it shows what the changes were.

No reports were available on the system at the time of the review that showed changes to supplier details. A trawl of creditor accounts was, therefore, undertaken (review of the first 100 accounts) to identify accounts that had undergone relevant changes (address or bank account changes only – other amendments, such as changes from orders being posted to emailed were not considered relevant).

Of the six accounts identified, supporting documentation was attached to the system in five cases. In the other case (which related to the bank account details being changed identified in the testing highlighted in 4.5.1 above), the amendment was queried with the person who had undertaken the change the Finance Administration Officer) and she was able to provide documentation that supported the change made.

4.6 Other Risks

4.6.1 Risk: Loss of IT / access to the Ci Anywhere finance management system.

The PAS advised that the system is a SAAS solution based in the cloud, so it is not under the remit of ICT Services for back up etc. with the server being held on Microsoft Azure and the solution being managed by Technology One (the company that owns Ci Anywhere).

4.6.2 Risk: Inappropriate access to Ci Anywhere.

As highlighted above, managers have to complete an access request form (which is available on the intranet) in order for staff to be given access to Ci Anywhere , although existing users of TOTAL had an equivalent access level granted without further authorisation being required.

The access levels are decided by the manager when they are requesting access, although the PAS suggested that they may query them if there are insufficient numbers of users with certain access levels within the department.

The (Accountancy) Systems Officer advised that access reviews are undertaken every six months, with users who have not accessed the system in that period having their account deactivated.

4.6.3 **Risk: Failure of BACS system leading to payments not being made to creditors.**

The SFAO advised that all cheque stocks had been destroyed.

In the event of a failure of BACS, the SFAO suggested that purchasing cards could be used (which may require amendments to card and transaction limits).

5 Summary and Conclusions

5.1 Section 3.2 sets out the risks that were under review as part of this audit. The review highlighted weaknesses against the following risks:

- Risk 4 – Incorrect payments are made (e.g. payments for the wrong amount / duplicate payments / goods not received etc.)
- Risk 5 - Discounts for prompt payment are not received / penalties for delayed payments are incurred.
- Risk 10 - Recovery action taken and / or loss of access to goods and services due to payments not being made in a timely manner.
- Risk 11 - Payments against valid creditor invoices are misappropriated.

5.2 A further 'issue' was also identified where an advisory note has been reported (see 4.2.5). In this instance, no formal recommendation is thought to be warranted, as there is no risk if the action is not taken.

5.3 In overall terms, however, we are able to give a SUBSTANTIAL degree of assurance that the systems and controls in place in respect of the Payment of Creditors are appropriate and are working effectively to help mitigate and control the identified risks.

5.4 The assurance bands are shown below:

Level of Assurance	Definition
Substantial	There is a sound system of control in place and compliance with the key controls.
Moderate	Whilst the system of control is broadly satisfactory, some controls are weak or non-existent and there is non-compliance with several controls.
Limited	The system of control is generally weak and there is non-compliance with controls that do exist.

6 Management Action

6.1 The recommendations arising above are reproduced in the attached Action Plan (Appendix A) for management attention.

6.2 Whilst section 5.1 highlights that there was a weakness against Risk 4, there is no related recommendation due to the ongoing attempts to rectify the situation.

Richard Barr
Audit and Risk Manager

Appendix A

Action Plan

Internal Audit of Payment of Creditors – March 2023

Report Ref.	Risk Area	Recommendation	Rating*	Responsible Officer(s)	Management Response	Target Date
4.2.5 / 4.4.2	Financial Risks - Discounts for prompt payment are not received / penalties for delayed payments are incurred. Reputational Risks - Recovery action taken and / or loss of access to goods and services due to payments not being made in a timely manner.	Staff should be reminded of the need to raise requisitions in a timely manner.	Low	Senior Finance Admin Officer	These issues can be covered by an annual e-mail to all users to remind them of the information. This email can also be used to target some of the common queries that we get from users.	30 April 2023
4.5.1	Fraud Risks – Payments against valid creditor invoices are misappropriated.	Staff should be reminded of the need to check bank account details recorded on the invoice against the standing data before a payment is made.	Medium			

* The ratings refer to how the recommendation affects the overall risk and are defined as follows:

High:	Issue of significant importance requiring urgent attention.
Medium:	Issue of moderate importance requiring prompt attention.
Low:	Issue of minor importance requiring attention.