



**FINAL INTERNAL AUDIT REPORT
CHIEF EXECUTIVE'S DEPARTMENT**

AUDIT REVIEW OF CREDITORS 2018/19

Issued to: Claudine Douglas-Brown, Assistant Director Exchequer Services
Emma Richardson, Head of Financial Systems
Lucinda Bowen, Head of Information Management

cc Peter Turner, Director of Finance

Prepared by: Senior Manager, (Audit contractor on behalf of London Borough of Bromley) and Senior Manager,
(Audit contractor on behalf of London Borough of Bromley)

Reviewed by: Principal Auditor and Head of Audit and Assurance

Date of Issue: 30 September 2019

Report No.: CEX/08/2018/AU

AUDIT REVIEW OF CREDITORS

INTRODUCTION

1. This report sets out the results of our audit of creditors. The audit was carried out as part of the work specified in the 2018-19 Internal Audit Plan agreed by the Section 151 Officer and Audit Sub-Committee. The controls we expect to see in place are designed to minimise the Council's exposure to a range of risks. Weaknesses in controls that have been highlighted will increase the associated risks and should therefore be addressed by management.
2. The Council's Exchequer contractor is contracted to provide the creditors service, which is delivered using the Oracle E Business Suite (EBS) (includes the iProcurement (or iProc) module and VersionOne). Information is also extracted from a number of Council maintained systems and MS Access databases to produce and validate payment requests for various services and petty cash reimbursements.
3. The Contract and Operations Team monitor the service provided by the Council's Exchequer contractor, as well as running various exception reports, such as the check for duplicate payments, and publishing the Council's expenditure for payments over £500 on the Council's website.
4. Support for the Oracle EBS, including user administration, is provided by the Financial Systems Team.
5. We would like to thank all staff contacted during this review for their help and co-operation.

AUDIT SCOPE

6. The original scope of the audit was outlined in the Terms of Reference and the following were considered to be the key risks inherent to the creditors' process:
 - Payments may be made for goods and services which have not been received.
 - Regular duplicate payment monitoring may not be undertaken and the results may not be actioned.
 - The creation, amendment and deletion of creditors master-file data may not be properly controlled.
 - iProc authority levels for the payments of goods and services may not be set and in line with Financial Regulations.
 - The number of retrospective iProc orders raised may not be identified and addressed.

AUDIT REVIEW OF CREDITORS

- Set-up / amendment forms for the creditors’ Masterfile may not be completed with a segregation of duties, or with an appropriate level of authority.
- The custody and handling of blank cheques may not be secure and properly controlled.
- The ledger control account may not be reconciled to the creditors’ control account.
- Payments may not be accurate or goods may not be received which may lead to refunds.

AUDIT OPINION

7. Our overall audit opinion, number and rating of recommendations are as follows.

AUDIT OPINION	
Limited Assurance	(Definitions of the audit assurance level and recommendation ratings can be found in Appendix B)

Number of recommendations by risk rating		
Priority 1	Priority 2	Priority 3
1	5	2

SUMMARY OF FINDINGS

8. Controls noted to be in place and working well, based on the audit testing conducted, include:

- The Council’s Financial Regulations and Procedures clearly detail the required procurement processes.
- The respective teams, namely the Contract and Operations Team, the Financial Systems Team and the Council’s Exchequer contractor have procedural guidance and checklists in place.

AUDIT REVIEW OF CREDITORS

- A Service Level Agreement (SLA) is in place with the Council's Exchequer contractor for the service provided.
- All the suppliers sampled were set up on iProc / Oracle upon receipt of appropriately completed forms and the setup and amendment of these suppliers was subject to a double check process.
- Checks are in place to help prevent and detect duplicate payments.
- Appropriate batch controls, including a supervisory check, are in place for the processing of invoice payments.
- Payments over £500 are published on the Council's website as required.
- Invoices, or other appropriate supporting documents, are scanned and retained for all the transactions sampled to support the payments made.
- Regular reconciliations of the creditors' control account are being undertaken.
- Monthly performance reports are being received from the Council's Exchequer contractor, in line with the agreed SLA.
- Appropriate security over manual cheques is in place.

9. We would like to bring to management attention the following issues:

- The supplier set up forms do not include a privacy statement and appropriate bank mandate checks are not in place.
- Authorised signatory forms are not properly completed and staff no longer engaged by the Council have not been removed from the listing.
- Users to the iProc module / Oracle system are being set up without reference to the authorised signatory list.
- We found that some orders were being raised retrospective to the invoices being received for payment and, although recommended in the previous audit report, reports of retrospective orders are not being run regularly.
- Transactions paid by the AP1 process do not meet the criteria specified in paragraphs 6.7 (i), (ii) and (iii) of Financial Regulations. It could not be demonstrated that these were exceptions as agreed by the Director of Finance because a list of such agreed exceptions was not readily available to the Council's Exchequer contractor.

AUDIT REVIEW OF CREDITORS

- The remittance advice printed and posted to suppliers in respect of 'CareFirst' type payments detailed client names. As these are sent by post to suppliers there is the risk of a data breach.
- There is no evidence that vacation rules are being applied to enable staff who are out of the office for a period of time to have their Oracle notifications and financial approval responsibilities assigned to a colleague.
- The guidance available on One Bromley for the use of iProc could be improved and there are no scheduled courses to train staff on iProc. We were informed that these would be provided if requested.

DETAILED FINDINGS / MANAGEMENT ACTION PLAN

10. The findings of this report, together with an assessment of the risk associated with any control weaknesses identified, are detailed in Appendix A. Any recommendations to management are raised and prioritised, together with management's responses and timescales for implementation. Appendix B details the definition of the audit assurance and priority ratings.

AUDIT REVIEW OF CREDITORS

DETAILED FINDINGS AND ACTION PLAN

APPENDIX A

No	Finding	Risk	Recommendation and Priority *Raised in previous Audit	Management Response	Agreed timescale and responsible manager
1	<p><u>Supplier set up procedures</u></p> <p>Please see the detailed findings set out at Appendix C to this report.</p>	<p>The Council is exposed to a number of risks, including those of inappropriate suppliers being set up and of mandate fraud.</p>	<p>Management should :</p> <p>(i) critically review the supplier set up process and</p> <p>(ii) in the interim, and as a matter of urgency, put processes in place to conduct robust bank mandate checks.</p> <p>Priority 1</p>	<p>The supplier set up process has been reviewed and the recommended changes have been implemented.</p>	<p>Assistant Director Exchequer Services</p> <p>Completed</p>
2	<p><u>Retrospective Orders</u></p> <p>The 2015/16 and 2017/18 internal audit reports both identified an issue with orders being raised retrospectively and recommended that a retrospective Purchase Orders report should be run on a regular basis.</p> <p>We confirmed with the Assistant Director Exchequer Services that the required report had not yet been formulated and thus the recommendation was not yet</p>	<p>Where purchase orders are raised retrospectively to invoices, the authorisation requirements are being bypassed and there is a risk that inappropriate purchases are made.</p>	<p>A retrospective Purchase Orders report should be run on a regular basis by a designated officer in Finance Directorate. The results should be provided to Directors, who should enquire from the relevant officer as to why an order was raised retrospectively.</p> <p>Priority 2</p>	<p>A retrospective Purchase Orders report will be run twice a year in October and March and the results will be provided to the Directors.</p>	<p>Contract and Operations Manager (Exchequer)</p> <p>31 October 2019</p>

AUDIT REVIEW OF CREDITORS

DETAILED FINDINGS AND ACTION PLAN

APPENDIX A

No	Finding	Risk	Recommendation and Priority *Raised in previous Audit	Management Response	Agreed timescale and responsible manager
	<p>actioned.</p> <p>Testing of a sample of payments identified for two of the six instances where iProc orders were raised, that these were retrospective (namely for order numbers 4208914 and 4209805)</p>				
3	<p><u>Remittance advice</u></p> <p>The Data Protection Act (DPA) 2018 requires that personal information is appropriately safeguarded and allows the Information Commissioner to levy significant fines for data breaches.</p> <p>We established that for all payments processed via CareFirst a remittance advice is printed and posted to the relevant care providers, which they are required to confirm and return. Subsequent payments to care providers will</p>	<p>There is a risk of a data breach and the Council consequently being fined under GDPR.</p>	<p>Management should ensure that :</p> <p>(i) The remittance advice for payments processed via CareFirst is amended to not detail personal information, (i.e. include a reference number instead of a client's name) and</p> <p>(ii) a more secure method of communicating the remittance advice between the Council and to the provider is put in place.</p> <p>Priority 2</p>	<p>A request has been made for the system provider OLM to amend the current remittance advice report to replace the full name with the client's initials.</p> <p>This is a standard report used by other OLM customers and we are waiting for a response from OLM regarding our options.</p> <p>In the meantime we will explore with IT Services whether the remittance advices can be processed between the Council and the providers by a more secure communication method</p>	<p>Assistant Director Exchequer Services and Head of information Management</p> <p>31 October 2019</p>

AUDIT REVIEW OF CREDITORS

DETAILED FINDINGS AND ACTION PLAN

APPENDIX A

No	Finding	Risk	Recommendation and Priority *Raised in previous Audit	Management Response	Agreed timescale and responsible manager
	<p>not be processed unless these remittances are returned. However, examination of a sample of remittance advices established that these detailed the client names.</p>			<p>i.e. secure email address.</p> <p>The specification for the replacement social care case management system will address the matter of GDPR compliance.</p>	
4	<p><u>Authorised Signatory List</u></p> <p>The Council's Financial Procedures paragraph 5.9 states that, '... The completed authorised signatory form should be forwarded to Accounts Payable (Resources Department) for them to hold in their records. Any changes should be notified immediately that they occur and not as a result of an update requested by Accounts Payable Department.'</p> <p>Examination of the completed</p>	<p>There is a risk that staff that have left the Council are still able to authorise transactions and that staff may be able to authorise transactions with a higher value than they should be able to.</p>	<p>Management should ensure that 'Corporate Authorised Signatories' forms should not be processed unless fully completed.</p> <p>Priority 2</p>	<p>The Council's Exchequer contractor has been reminded that any Authorised Signatories forms that have not been fully or accurately completed should be rejected.</p> <p>The Council's Exchequer contractor will now receive a monthly list of employees who have left the authority and will update the Authorised Signatory list.</p>	<p>Assistant Director Exchequer Services</p> <p>Completed</p>

AUDIT REVIEW OF CREDITORS

DETAILED FINDINGS AND ACTION PLAN

APPENDIX A

No	Finding	Risk	Recommendation and Priority *Raised in previous Audit	Management Response	Agreed timescale and responsible manager
	<p>'Corporate Authorised Signatories' forms for a sample of 5 staff added to the Council in 2019 found that 3 of these forms did not detail the financial limit delegated. It was explained that, unless the signatory form was for an Assistant Director or Director, that the maximum allowable delegated amount of £99,999 would be applied.</p> <p>Examination of the authorised signatory database for a sample of 27 staff that had transferred to Amey from the Council found that 17 of these staff were still on the Council's authorised signatory list - We are aware that this is also being addressed separately through recommendations about the process for the timely removal of leavers made in the audit of 'starters and leavers'.</p>				

AUDIT REVIEW OF CREDITORS

DETAILED FINDINGS AND ACTION PLAN

APPENDIX A

No	Finding	Risk	Recommendation and Priority *Raised in previous Audit	Management Response	Agreed timescale and responsible manager
5	<p><u>Access to Oracle / iProc</u></p> <p>In order to obtain access to Oracle / iProc), staff are required to complete the 'New iProc User' form.</p> <p>We established that the staff who process the 'New iProc user' forms and set new users up on the system do not have access to or sight of the Council's authorised signatory list. For two of the sample of new users examined, the iProc limits assigned differed to the authorised signatory list delegated limit, (in both cases the iProc limit was far less).</p> <p>Furthermore, examination of the user accounts for a sample of five staff who had moved to Amey from the Council found that three of these users were still enabled, although assurances were provided that these users would not be able to access the system - We are</p>	<p>There is a risk that staff who are not on the Council's authorised signatory list obtain access to Oracle, staff remain set up on iProc after they have left the Council, or that the financial limits applied are not in accordance with those detailed in the authorised signatory list.</p>	<p>Management should ensure that:</p> <p>(i) new iProc users or changes to iProc user accounts should only be set up and processed if in accordance with the Council's authorised signatory list and</p> <p>(ii) the iProc accounts of staff who have left should be properly disabled.</p> <p>Priority 2</p>	<p>We will ensure that new iProc user accounts or changes to existing users' accounts are set up and processed in line with the Council's authorised signatory list.</p> <p>When a user's Oracle account is disabled, this action also disables the iProc access of their Oracle account, meaning that they no longer have ability to raise or approve orders. Their iProc set up however remains on the system until it is disabled separately. We will therefore identify all former employees who still have iProc set up on the system and disable it.</p>	<p>Head of Financial Systems</p> <p>31 October 2019</p>

AUDIT REVIEW OF CREDITORS

DETAILED FINDINGS AND ACTION PLAN

APPENDIX A

No	Finding	Risk	Recommendation and Priority *Raised in previous Audit	Management Response	Agreed timescale and responsible manager
	<p>aware that this is being addressed separately through recommendations about the process for the timely removal of IT access for leavers made in the audit of 'starters and leavers'.</p>				
6	<p><u>Use of AP1 payment forms</u></p> <p>The Council's Financial Regulations and Procedures paragraph 6.4 details that, 'All orders should be raised on the iProc system. Where this is not possible, unique pre-numbered official hard copy orders should be raised, any exceptions should be agreed by the Director of Finance'; and paragraph 6.7 details that, 'An official order, or its equivalent, must be raised for all goods, works and services except where one or more of the following apply:</p> <p>(i) Where a specific formal</p>	<p>There is a risk that transactions are processed on AP1's rather than as required on iProc.</p>	<p>The use of AP1 payment forms to process transactions that do not meet the criteria specified in Paragraph 6.7 (1), (ii) and (iii) of the Financial Regulations and Procedures should be critically reviewed.</p> <p>A list of exceptions as agreed by the Director of Finance should be made available to the Council's Exchequer contractor staff to enable them to manage the use of AP1's.</p> <p>Priority 2</p>	<p>A list of exceptions as agreed by the Director of Finance will be made available to the Council's Exchequer contractor staff to enable them to manage the use of AP1's. Any that do not comply with Financial Regulations will be returned to the certifying officer.</p>	<p>Assistant Director Exchequer Services</p> <p>31 October 2019</p>

AUDIT REVIEW OF CREDITORS

DETAILED FINDINGS AND ACTION PLAN

APPENDIX A

No	Finding	Risk	Recommendation and Priority *Raised in previous Audit	Management Response	Agreed timescale and responsible manager
	<p>contract exists which does not incorporate any facility for the regular draw-down of services;</p> <p>(ii) Rents, business rates, council tax and utility services as supplies of a continuous and obligatory nature;</p> <p>(iii) Petty cash payments.’</p> <p>Examination of a sample of AP1 batches identified instances where payments were being made that did not meet the criteria specified in Paragraph 6.7 (i), (ii) and (iii) of the financial procedures. It could not be confirmed by the Council’s Exchequer contractor staff whether these transactions were exceptions as agreed by the Director of Finance, as they did not have access to any listing of agreed exemptions.</p>				

AUDIT REVIEW OF CREDITORS

DETAILED FINDINGS AND ACTION PLAN

APPENDIX A

No	Finding	Risk	Recommendation and Priority *Raised in previous Audit	Management Response	Agreed timescale and responsible manager
7	<p><u>iProc guidance and training</u></p> <p>We confirmed that general guidance on procurement is available in the Council's Financial Regulations and Procedures and that relevant forms are readily available on the One Bromley SharePoint site (i.e. AP1, AP2, authorised signatory and supplier set up forms). However, there is a lack of general guidance on the use of iProc or links to other relevant guidance, (for example HMRC self-employed and IR35 rules or the Council's tender and quote requirements, although we are aware that the Council's Financial Regulations and Procedures and Contract Procedure Rules are currently being reviewed).</p> <p>It was also confirmed that training on the use of the iProc system would be provided if</p>	<p>There is a risk that staff may not comply with the required iProc procedures.</p>	<p>Management should review the general guidance and training available to staff on the use of iProc, to help ensure that staff comply with expected controls and achieve desired objectives.</p> <p>Priority 3</p>	<p>We will liaise with the Assistant Director Governance & Contracts because the governance of iProc was the responsibility of the previous Head of Corporate Procurement. Appropriate guidance and training will then be put in place.</p>	<p>Head of Financial Systems</p> <p>30 November 2019</p>

AUDIT REVIEW OF CREDITORS

DETAILED FINDINGS AND ACTION PLAN

APPENDIX A

No	Finding	Risk	Recommendation and Priority *Raised in previous Audit	Management Response	Agreed timescale and responsible manager
	requested. There was, however, no scheduled training available.				
8	<p><u>Vacation rules</u></p> <p>Oracle allows vacation rules to be set whilst staff are out of the office for a period of time, which allows them to delegate to another person to receive their Oracle notifications and approval responsibility. However, when delegated to more junior members of staff, this allows the authorised signatory delegated limits to be by-passed.</p> <p>Management were not able to confirm whether vacation rules were enabled or not.</p>	<p>There is a risk that authorised signatory delegated limits may be by-passed.</p>	<p>Management should confirm whether vacation rules are enabled or not and controls should be put in place to ensure that authorised signatory delegated limits are not by-passed.</p> <p>Priority 3</p>	<p>We will explore the option of putting in place vacation rules and examine what controls can be put in place to ensure that authorised signatory delegated limits are not by-passed.</p>	<p>Head of Financial Systems</p> <p>30 November 2019</p>

Assurance Level

Assurance Level	Definition
Substantial Assurance	There is a sound system of control in place to achieve the service or system objectives. Risks are being managed effectively and any issues identified are minor in nature.
Reasonable Assurance	There is generally a sound system of control in place but there are weaknesses which put some of the service or system objectives at risk. Management attention is required.
Limited Assurance	There are significant control weaknesses which put the service or system objectives at risk. If unresolved these may result in error, abuse, loss or reputational damage and therefore require urgent management attention.
No Assurance	There are major weaknesses in the control environment. The service or system is exposed to the risk of significant error, abuse, loss or reputational damage. Immediate action must be taken by management to resolve the issues identified.

Recommendation ratings

Risk rating	Definition
Priority 1	A high priority finding which indicates a fundamental weakness or failure in control which could lead to service or system objectives not being achieved. The Council is exposed to significant risk and management should address the recommendation urgently.
Priority 2	A medium priority finding which indicates a weakness in control that could lead to service or system objectives not being achieved. Timely management action is required to address the recommendation and mitigate the risk.
Priority 3	A low priority finding which has identified that the efficiency or effectiveness of the control environment could be improved. Management action is suggested to enhance existing controls.

Recommendation 1 – detailed findings

Supplier set up procedures

The Accounts Payable Service Level Requirements document, dated June 2016, between the Council and the Service Provider, i.e. The Council's Exchequer contractor paragraph 1.1.16 details that, 'The Service Provider will process requests to set up new suppliers and to amend existing suppliers' details...'.

In order for new suppliers to be set up or be amended, a 'Supplier Setup / Amendment Form' is required to be completed, section 1 by the relevant Council Service and sections 2, 3 and 4 by the supplier. As new suppliers may include individuals, who are providing personal data, the form should include a suitable 'privacy statement' to comply with the transparency requirements of the Data Protection Act 2018. It does not, however, include this.

Upon receipt of the completed form and after checking to confirm that the supplier does not already exist, the 'Supplier Management' Team within the Council's Exchequer contractor will set up the new supplier.

The 2017/18 internal audit report on creditors included a Priority 1 recommendation that 'before the supplier Setup / Amendment form is processed, it is checked and authorised by a budget holder or other designated manager'.

This check is not evidenced and, with a number of completed 'Supplier Setup / Amendment Forms' being e-mailed directly from suppliers to the 'Supplier Management' Team, the check does not occur in a number of cases.

Furthermore, with a lack of guidance to budget holders or designated managers, it is uncertain whether these officers are aware of the requirement to check completed 'Supplier Setup / Amendment Forms', or if they did so, what to check.

Where the supplier is VAT registered, this will be checked to the European Commission Taxation and Customs Union regulations and where the supplier is CIS (Construction Industry Scheme), the Unique Tax Reference and the Company Number will be checked by the 'Supplier Management' Team.

We found that no further checks, including those to verify the bank account details being provided, are conducted.