

ABERDEEN CITY COUNCIL

---

<b>COMMITTEE</b>	Audit, Risk and Scrutiny Committee
<b>DATE</b>	08 May 2025
<b>EXEMPT</b>	No
<b>CONFIDENTIAL</b>	No
<b>REPORT TITLE</b>	Internal Audit Report AC2506 – Creditors Sub-System Payments
<b>REPORT NUMBER</b>	IA/AC2506
<b>DIRECTOR</b>	N/A
<b>REPORT AUTHOR</b>	Jamie Dale
<b>TERMS OF REFERENCE</b>	2.2

---

**1. PURPOSE OF REPORT**

- 1.1 The purpose of this report is to present the planned Internal Audit report on Creditors Sub-System Payments.

**2. RECOMMENDATION**

- 2.1 It is recommended that the Committee review, discuss and comment on the issues raised within this report and the attached appendix.

**3. CURRENT SITUATION**

- 3.1 Internal Audit has completed the attached report which relates to an audit of Creditors Sub-System Payments.

**4. FINANCIAL IMPLICATIONS**

- 4.1 There are no direct financial implications arising from the recommendations of this report.

**5. LEGAL IMPLICATIONS**

- 5.1 There are no direct legal implications arising from the recommendations of this report.

**6. ENVIRONMENTAL IMPLICATIONS**

- 6.1 There are no direct environmental implications arising from the recommendations of this report.

**7. RISK**

- 
- 7.1 The Internal Audit process considers risks involved in the areas subject to review. Any risk implications identified through the Internal Audit process are detailed in the resultant Internal Audit reports. Recommendations, consistent with the Council's Risk Appetite Statement, are made to address the identified risks and Internal Audit follows up progress with implementing those that are agreed with management. Those not implemented by their agreed due date are detailed in the attached appendices.

## **8. OUTCOMES**

- 8.1 There are no direct impacts, as a result of this report, in relation to the Council Delivery Plan, or the Local Outcome Improvement Plan Themes of Prosperous Economy, People or Place.
- 8.2 However, Internal Audit plays a key role in providing assurance over, and helping to improve, the Council's framework of governance, risk management and control. These arrangements, put in place by the Council, help ensure that the Council achieves its strategic objectives in a well-managed and controlled environment.

## **9. IMPACT ASSESSMENTS**

<b>Assessment</b>	<b>Outcome</b>
<b>Impact Assessment</b>	An assessment is not required because the reason for this report is for Committee to review, discuss and comment on the outcome of an internal audit. As a result, there will be no differential impact, as a result of the proposals in this report, on people with protected characteristics.
<b>Privacy Impact Assessment</b>	Not required

## **10. BACKGROUND PAPERS**

- 10.1 There are no relevant background papers related directly to this report.

## **11. APPENDICES**

- 11.1 Internal Audit report AC2506 – Creditors Sub-System Payments

## **12. REPORT AUTHOR CONTACT DETAILS**

<b>Name</b>	Jamie Dale
<b>Title</b>	Chief Internal Auditor
<b>Email Address</b>	<a href="mailto:Jamie.Dale@aberdeenshire.gov.uk">Jamie.Dale@aberdeenshire.gov.uk</a>
<b>Tel</b>	(01467) 530 988



## Internal Audit

### Assurance Review of Creditors Sub-System Payments

**Status:** Final

**Date:** 31 March 2025

**Risk Level:** Cluster

**Report No:** AC2506

**Assurance Year:** 2024/25

Net Risk Rating	Description	Assurance Assessment
<b>Moderate</b>	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified, which may put at risk the achievement of objectives in the area audited.	<b>Reasonable</b>

Report Tracking	Planned Date	Actual Date
Scope issued	09-Oct-24	09-Oct-24
Scope agreed	16-Oct-24	17-Oct-24
Fieldwork commenced	28-Oct-24	12-Nov-24
Fieldwork completed	22-Nov-24	06-Dec-24
Draft report issued	13-Dec-24	20-Dec-24
Process owner response	17-Jan-25	04-Mar-25
Director response	24-Jan-25	28-Mar-25
Final report issued	31-Jan-25	31-Mar-25
ARS Committee	08-May-25	

Distribution	
<b>Document type</b>	Assurance Report
<b>Directors</b>	Andy MacDonald, Executive Director – Corporate Services
<b>Process Owner</b>	Bernadette Bularan, Deputy Chief Finance Officer
<b>Stakeholders</b>	Jonathan Belford, Chief Officer – Finance
	Lesley Fullerton, Finance Operations Manager
	Angela Crawford, Finance Controls Manager
	Richard Burnett, Senior Accountant
	Steve Roud, Chief Officer – Digital & Technology
	Lesley Strachan, Service Lead - People Services
	Andrea Garden, Team Leader – Payroll
	Vikki Cuthbert, Interim Chief Officer - Governance
	External Audit*
<b>*Final Only</b>	
<b>Lead auditor</b>	Agne McDonald, Auditor

---

# 1 Introduction

## 1.1 Area subject to review

The Council uses the Creditors System within their financial management system (eFinancials) to make payments to its suppliers. During 2023/24, 438,716 creditor payments totalling £898.844 million were made. Of this, 87,165 totalling £399.186 million (44%) were processed from eight feeder systems which process invoices / remittances out with the eFinancials Creditors system. These feeder systems are:

1. Confirm – non-HRA property repairs
2. Firmstep – education maintenance allowance / school clothing grants
3. Spydus – library management system
4. Total – HRA building maintenance and roads
5. CorePay – payroll creditors payments
6. Key2 – vehicle maintenance and hire vehicles
7. D365 – social work care packages
8. NDR – refunds of business rates

In addition, various payments are processed via manual bulk payment where spreadsheet based bulk payment files require to be submitted to the Financial Systems Team (FST) following approval by the relevant budget holder. This includes for example kinship/adoption payments; nursery milk payments; and Early Learning and Childcare (ELC) provider payments.

Payment text files are generated from the feeder systems above, either as part of a scheduled automated process, or when instigated by the relevant feeder system administration staff. Similarly, Accounts Payable staff are responsible for generating the BACS payment text file from eFinancials so payment can be processed via the BACS system.

The Financial Systems Team is responsible for ensuring the accuracy of interface files uploaded to the Council's financial management system and for reconciling creditor payments made to the Council's bank account.

## 1.2 Rationale for review

The objective of this audit is to provide assurance that there are adequate controls over payments originating from creditors sub-systems.

The last full Internal Audit review of this area took place in August 2018 as part of Internal Audit AC1901 Creditor Payments when recommendations were agreed to improve written procedures; reconciliation arrangements; payment control; and limit privileged access rights. More recently Internal Audit AC2203 Financial Systems Interfaces and Reconciliations and AC2407 Creditors System carried out in November 2021 and May 2024 respectively, covered accounts payable interface and payment control processes, with recommendations agreed to restrict and monitor privileged user access (including manual adjustments to payment files); to control changes to supplier standing data affecting payments; and to enhance BACS reconciliation procedures.

This audit has been included in the agreed Internal Audit plan for 2024/25 due to the material value of payments being interfaced from sub-systems into the Creditors System and the risk of fraudulent payments if internal controls are inadequate. For example, in 2016/17, another Scottish Local Authority identified a significant fraud perpetrated by a long serving member of staff, with extensive access to several Council systems. They combined their knowledge of these systems with their unrestricted system access privileges, to insert fictitious invoices into the Creditors System for payment. This fraud perpetrated over a number of years resulted in over £1m of fraudulent payments.

## 1.3 How to use this report

This report has several sections and is designed for different stakeholders. The executive summary (section 2) is designed for senior staff and is cross referenced to the more detailed narrative in later sections (3 onwards) of the report should the reader require it. Section 3 contains the detailed narrative for risks and issues we identified in our work.

## 2 Executive Summary

### 2.1 Overall opinion

The full chart of net risk and assurance assessment definitions can be found in Appendix 1 – Assurance Scope and Terms. We have assessed the net risk (risk arising after controls and risk mitigation actions have been applied) as:

Net Risk Rating	Description	Assurance Assessment
<b>Moderate</b>	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified, which may put at risk the achievement of objectives in the area audited.	<b>Reasonable</b>

The organisational risk level at which this risk assessment applies is:

Risk Level	Definition
<b>Cluster</b>	This issue / risk level impacts a particular Service or Cluster. Mitigating actions should be implemented by the responsible Chief Officer.

### 2.2 Assurance assessment

The level of net risk is assessed as **MODERATE**, with the control framework deemed to provide **REASONABLE** assurance over the Council's approach to Creditors Sub-System Payments.

The Council uses the Creditors System within their Financial Management System to make payments to its suppliers.

During 2023/24, 438,716 creditor payments totalling £898.844 million were made. Of this, 87,165 totalling £399.186 million (44%) were processed from eight feeder systems which process invoices / remittances out with the eFinancials Creditors system. One of these sub-systems is used for processing Education Maintenance Allowances and clothing grants – this was not subject to review as it was covered recently in AC2501 – Allowances.

In addition, various payments are processed via manual bulk payment where spreadsheet based bulk payment files require to be submitted to the Financial Systems Team (FST) following approval by the relevant budget holder. Early Learning and Childcare (ELC) provider payments and nursery milk payments were not covered when testing bulk payments since they were reviewed in reports AC2501 – ELC Funded Provider Places; and AC2312 – Scottish Milk and Health Snack Scheme respectively.

Reasonable assurance was available over the following areas reviewed:

- **Written Procedures** – Finance has detailed written procedures in place covering the processing of creditors interfaces from feeder sub-systems and related reconciliation arrangements.
- **Finance Interface Verification** – The Financial Systems Team (FST) checks to ensure that creditor sub-system payment files received are successfully uploaded to the Council's creditors system, with any rejections being notified back to the feeder sub-system Service for correction. The FST maintain a batch register to assist with this process.
- **BACS reconciliations** – BACS run payment values within the BACS system are being reconciled to the creditors system using Business Objects reporting on the creditors system and PTX BACS submission summary reports. A sample of five consecutive days of BACS submissions in December 2024 was fully supported with no reconciling differences.

However, the review identified some areas of weakness where enhancements could be made to strengthen the framework of control, specifically:

- **Delegated Authority** – In breach of the Council's Scheme of Governance, authorisation limits within the Council's corporate purchase ordering and invoice authorisation systems are being determined by line managers, team leaders or budget holders instead of chief officers as required. Also, Finance has advised that sub-system authorisation limits are not aligned with

the corporate purchasing ordering and invoice authorisation system limits risking inconsistency. Where purchase order and payment authorisation systems have incomplete, inconsistent and unauthorised approval limits, which are not linked to authority delegated from chief officers, there is a greater risk of unauthorised payments, payment error and potentially fraud. In addition, the Council's Financial Regulations only permit electronic authorisation of payments within the corporate invoice authorisation system. However, all 30 sub-system payments reviewed were approved electronically out with this system in breach of Financial Regulations.

- **Sub-System Owner Interface Checking** – Reconciliations of payments uploaded to the creditors system are not currently completed by sub-system owners/administrators or relevant staff within the sub-system originating service. Whilst reports are available to FST staff to undertake checks of payment file upload success, relevant sub-system service officers do not have their own independent access to such reports for reconciliation purposes. The FST staff have privileged access to the creditors system and interface files, meaning they can make changes that can affect payments. Independent scrutiny of payment file upload accuracy would be beneficial to further reduce the risk of payment error and reduce the risk of fraud. More generally, a recommendation has already been made as part of Internal Audit report AC2407 Creditors System to monitor privileged user activity, including supplier bank account creation and amendments.
- **Payroll Creditors Interfaces** – Whilst 27 (90%) uploaded creditors sub-system payment batches reviewed, across seven sub-systems, had all been agreed to payment batch control totals from the sub-system by the FST, three (10%) payroll creditors batches relating to employee payroll deductions were not since this information is not available to the FST. This gap impedes control over interface accuracy and increases the risk of incomplete or inaccurate payments.
- **BACS Procedure** – The BACS procedure is detailed and clear, with system screenshots, describing the necessary steps to process BACS payments and some basic instructions for completing the related reconciliation. However, it was noted that the procedure does not specify who can undertake the BACS reconciliation presenting a minor risk an FST member, with privileged system access, may undertake a check of files they have processed in future, invalidating the check. In addition, the BACS procedure includes details of a shared password for Business Objects reports showing BACS details; this should be addressed as sharing passwords is contrary to the Council's Corporate ICT Acceptable Use Policy.
- **Payment Control** – Bank account evidence was absent for two (7%) of 27 payments across seven sub-systems reviewed risking fraud or payment error. Where bank accounts used for payments were supported, the adequacy of related evidence was not assessed as part of this review since a recommendation has already been agreed as part of Internal Audit report AC2407 Creditors System to standardise payee identification and bank account evidence requirements.

Recommendations have been made to address the above risks, including establishing a standardised, and published delegated authority list for purchase order and payment authorisations, aligned to job responsibilities and ensuring purchase ordering and payment systems are aligned to this; introducing sub-system owner checks of uploaded payments; and establishing payroll creditors interface checks by Finance back to the payroll system. In addition, a recommendation was made to update the BACS procedure.

## 2.3 Severe or major issues / risks

Issues and risks identified are categorised according to their impact on the Council. The following are summaries of higher rated issues / risks that have been identified as part of this review:

Ref	Severe or Major Issues / Risks	Risk Agreed	Risk Rating	Page No.
1.3	<b>Delegated Authority</b> – Chief officers have delegated authority to approve officer signatory lists and officer authorisation levels in relation to the raising and approval	Yes	<b>Major</b>	11

Ref	Severe or Major Issues / Risks	Risk Agreed	Risk Rating	Page No.
	<p>of purchase orders and the authorisation of payments.</p> <p>Whilst this authority is delegated to chief officers, the authority to approve purchase orders and payments and associated authorisation levels within the corporate purchase ordering system and invoice authorisation system is determined by an employee's line manager, team leader, or the respective budget holder and not the chief officer in breach of the Council's Scheme of Governance.</p> <p>Since corporate purchase ordering and invoice authorisation systems are not linked to chief officer delegated authority, this is a major gap in the system of payment control.</p> <p>A sample of 27 payments across seven sub-systems and three payments processed via manual bulk payment uploads were reviewed. Based on the corporate invoice authorisation system limits, two (14%) sub-system approvals totalling £6k were by officers without delegated authority, one (3%) invoice approved exceeded the approver's value limit by £168k and for another (3%) low value approval of £400, it was not clear if authority existed since an approval limit had not been set within the corporate invoice authorisation system, despite it being appropriate to do so for payment control purposes.</p> <p>Finance advised sub-system authorisation levels are not aligned with the corporate invoice authorisation system authorisation levels risking authorisation inconsistency.</p> <p>Where purchase order and payment authorisation systems have incomplete, inconsistent and unauthorised approval limits, which are not linked to authority delegated from chief officers, there is a greater risk of unauthorised payments, payment error and potentially fraud.</p>			

## 2.4 Management response

*The Council Management appreciates the efforts and findings shared by the Internal Audit Team on this subject. Noting the objective of this audit, i.e. provide assurance that there are adequate controls over payments originating from creditors sub-systems, due attention has to be given on all relevant feeder systems where the payment requisitions originate from in terms of their procedures / authorisation levels and settings / documentation supports. It is worth noting the Financial Regulation clause 3.2 holding each Service Lines' Chief Officers to account as follows: "Chief Officers are responsible for the submission of a Certificate of Assurance on the Effectiveness of Internal Financial Controls to the Chief Officer – Finance on an annual basis." Based on this premise, payment*

---

*requisitions from each Service Lines will need to have due diligence and control in place prior to the final payment release done via the Creditors System to meet that level of assurance due.*



### 3 Issues / Risks, Recommendations, and Management Response

#### 3.1 Issues / Risks, recommendations, and management response

Ref	Description	Risk Rating	Moderate
1.1	<p><b>Written Procedures and Guidance</b> – Comprehensive written procedures and guidance, which are easily accessible by relevant members of staff, can reduce the risk of errors and inconsistency. They provide management with assurance correct and consistent instructions are available, especially in the event of an experienced employee being absent or leaving.</p> <p>The BACS procedure is detailed and clear, with system screenshots, describing the necessary steps to process BACS payments and some basic instructions for completing the related reconciliation.</p> <p>However, it was noted that the procedure does not specify who can undertake the BACS reconciliation, presenting a risk an FST member, with privileged system access, may in future undertake a check of files they have processed, invalidating the check.</p> <p>In addition, the BACS procedure includes details of a shared password for Business Objects reports showing BACS details. This is contrary to both the Council's ICT Acceptable Use Policy and the Council's ICT Access Control Policy, with the latter stating, <i>"passwords must never be shared"</i>.</p> <p>This should be addressed to mitigate the risk of unauthorised access to BACS payment data via Business Objects and to comply with Council policy.</p> <p><b>IA Recommended Mitigating Actions</b></p> <p>The BACS procedure should be reviewed and updated where necessary.</p> <p><b>Management Actions to Address Issues/Risks</b></p> <p><i>Management agrees with the IA recommendation that the BACS Procedures be reviewed, mapped, and updated.</i></p>		
Risk Agreed	Person(s)	Due Date	
Yes	Finance Operations Manager	October 2025	

Ref	Description	Risk Rating	Moderate
1.2	<p><b>Interfaces</b> – Where payment data is transferred between two systems, a system of control is required to ensure the data transferred is accurate and complete and that no manual amendments have been made that would increase the risk of error and fraud. There are eight feeder sub-systems which process invoices/payments out with the creditors system. Payment text files are generated from these feeder systems, either as part of a scheduled automated process, or when instigated by the relevant feeder system administration staff. Four "sub-systems" rely on manual spreadsheet based bulk payment processing (Kickstart Grants, Kinship/Adoption Payments, Nursery Milk Payments and ELC Provider payments).</p> <p>Education Maintenance Allowance, Clothing Grant, Nursery Milk, and ELC Funded Provider sub-system payments have not been subject to review as part of this audit, since these payments have been covered recently by Internal Audit in standalone reviews.</p>		

Ref	Description	Risk Rating	Moderate
	<p>Kinship/Adoption payments were tested as part of this audit to review related interface controls.</p> <p><u>Finance Interface Checking</u></p> <p>For a sample of thirty payment batches reviewed, whilst 27 (90%) uploaded creditors sub-system payment batches reviewed, across seven sub-systems, had all been agreed to payment batch control totals from the sub-system by the FST, three (10%) payroll creditors batches relating to employee payroll deductions were not since this information is not available to the FST.</p> <p>Upon inquiry, the Financial Systems Team (FST) confirmed that this data is not provided by Payroll. Whilst this is partially mitigated by the FST reconciling the batch values to interface details within the creditors system interface “clink” holding area, provided by ICT each morning, there is no confirmation of totals back to the sub-system (i.e. independent of the creditors system). This gap increases the risk of incomplete or inaccurate payments.</p> <p><u>Sub-System Owner Interface Checking</u></p> <p>Reconciliations of payments uploaded to the creditors system are not currently completed by sub-system owners / administrators or relevant staff within the sub-system originating service. Whilst reports are available to FST staff to undertake checks of payment file upload success, relevant sub-system service officers do not have their own independent access to such reports for reconciliation purposes. The FST staff have privileged access to the creditors system and interface files, meaning they can make changes that can affect payments. Independent scrutiny of payment file upload accuracy would be beneficial to further reduce the risk of payment error and reduce the risk of fraud.</p> <p>The above interface reconciliation issues, reduce control over the accuracy, completeness and existence of payments processed which increases the risk of payment error and potentially fraud.</p>		
<b>IA Recommended Mitigating Actions</b>			
<p>a) Payroll should enhance payroll creditors interface reporting to enable the Financial Systems Team (FST) to gain assurance over the accuracy and completeness of uploaded payroll creditors payment files.</p> <p>b) Finance should grant relevant sub-system staff access to creditors system reports necessary to reconcile sub-system payments to the creditors system and provide instruction on the requirement to verify payment upload accuracy. Any creditors system reports should be accessible without intervention from the FST. Reports should also be made available to staff within the sub-system service without administrator / superuser access to the sub-system for oversight purposes.</p>			
<b>Management Actions to Address Issues/Risks</b>			
<p>a) Agreed.</p> <p>b) Finance will review this recommended mitigating action and act accordingly. Currently, the Finance Team provides reconciliation reports to the sub-system staff for the latter's review and actions; and any additional clarifications from sub-system staff are being attended to.</p>			
<b>Risk Agreed</b>	<b>Person(s)</b>	<b>Due Date</b>	
a) Yes	a) Senior Development Officer	a) Implemented	
b) Yes	b) Finance Operations Manager in collaboration with the Senior Accountant (or FST Team Lead) and the	b) December 2025	

Ref	Description	Risk Rating	Moderate
	Feeder Systems System Administrators and Users		

Ref	Description	Risk Rating	Major
1.3	<p><b>Delegated Authority</b> – The Council's List of Officer Powers states under the General Delegations to Chief Officers [Chief Officers have the power]:</p> <p><i>"To approve purchase orders and authorise payments; and to approve officer signatory lists and officer authorisation levels in relation to the raising and approval of purchase orders and the authorisation of payments."</i></p> <p>Finance advised that a central delegated authority list is maintained within the corporate invoice authorisation system.</p> <p>However, this authorisation list, which is used for the authorisation levels within the corporate purchase ordering system and invoice authorisation system, is determined by an employee's line manager, team leader, or the respective budget holder and not the Chief Officer, in breach of the Council's Scheme of Governance. The authorisation levels within the corporate purchase ordering and invoice authorisation systems are therefore incorrect.</p> <p>Since corporate purchase ordering and invoice authorisation systems are not linked to chief officer delegated authority, this is a major gap in the system of payment control.</p> <p>A sample of 27 payments across seven sub-systems and three payments processed via manual bulk payment uploads were reviewed. 14 (47%) of the 30 payment approvers reviewed were present on Finance's invoice authorisation system authorised signatory list. According to the invoice authorisation system authorisation list, two (7%) invoice approvals totalling £6k were by officers without delegated authority, one (3%) invoice approved exceeded the approver's value limit by £168k and for another (3%) lower value approval of £400, it was not clear if authority existed for a Service Manager since an approval limit had not been set, despite it being appropriate to do so for payment control purposes.</p> <p>Furthermore, Finance advised sub-system authorisation levels are not aligned with the corporate invoice authorisation system authorisation levels risking authorisation inconsistency.</p> <p>Where purchase order and payment authorisation systems have incomplete, inconsistent and unauthorised approval limits, which are not linked to authority delegated from chief officers, there is a greater risk of unauthorised payments, payment error and potentially fraud.</p> <p>The Council's Financial Regulations also state:</p> <p><i>"Invoices must be processed for payment in accordance with the supplier's credit terms with expenditure authorised by authorised signatories (electronically through PECOS / Infosmart or with original signature)."</i></p> <p>However, all 27 payments reviewed totalling £334k, which were processed outwith PECOS / Infosmart via creditor sub-systems, were not approved by an original signature in breach of Financial Regulations.</p> <p><b>IA Recommended Mitigating Actions</b></p> <p>a) The Council's purchase order and payment authorised signatory lists and related authorisation levels should be standardised by job responsibilities, approved by chief officers</p>		

Ref	Description	Risk Rating	Major
	and published. Purchase order and payment authorisation systems should then be updated to ensure authorisation limits are aligned with delegated authority. b) Finance should review "original signature" requirements within Financial Regulations and either instruct authorised signatories to comply with the requirements or revise Financial Regulations to permit electronic payment authorisation outwith PECOS / Infosmart.		
	<b>Management Actions to Address Issues/Risks</b>		
	a) Agreed. b) Agreed.		
	<b>Risk Agreed</b>	<b>Person(s)</b>	<b>Due Date</b>
	a) Yes	Finance Operations Manager	December 2025
	b) Yes		

## 4 Appendix 1 – Assurance Terms and Rating Scales

### 4.1 Overall report level and net risk rating definitions

The following levels and ratings will be used to assess the risk in this report:

Risk level	Definition
<b>Corporate</b>	This issue / risk level impacts the Council as a whole. Mitigating actions should be taken at the Senior Leadership level.
<b>Function</b>	This issue / risk level has implications at the functional level and the potential to impact across a range of services. They could be mitigated through the redeployment of resources or a change of Policy within a given function.
<b>Cluster</b>	This issue / risk level impacts a particular Service or Cluster. Mitigating actions should be implemented by the responsible Chief Officer.
<b>Programme and Project</b>	This issue / risk level impacts the programme or project that has been reviewed. Mitigating actions should be taken at the level of the programme or project concerned.

Net Risk Rating	Description	Assurance Assessment
<b>Minor</b>	A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.	<b>Substantial</b>
<b>Moderate</b>	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified, which may put at risk the achievement of objectives in the area audited.	<b>Reasonable</b>
<b>Major</b>	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.	<b>Limited</b>
<b>Severe</b>	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.	<b>Minimal</b>

Individual Issue / Risk Rating	Definitions
<b>Minor</b>	Although the element of internal control is satisfactory there is scope for improvement. Addressing this issue is considered desirable and should result in enhanced control or better value for money. Action should be taken within a 12 month period.
<b>Moderate</b>	An element of control is missing or only partial in nature. The existence of the weakness identified has an impact on the audited area's adequacy and effectiveness. Action should be taken within a six month period.
<b>Major</b>	The absence of, or failure to comply with, an appropriate internal control, which could result in, for example, a material financial loss. Action should be taken within three months.
<b>Severe</b>	This is an issue / risk that could significantly affect the achievement of one or many of the Council's objectives or could impact the effectiveness or efficiency of the Council's activities or processes. Action is considered imperative to ensure that the Council is not exposed to severe risks and should be taken immediately.

---

## 5 Appendix 2 – Assurance review scoping document

### 5.1 Area subject to review

The Council uses the Creditors System within their financial management system (eFinancials) to make payments to its suppliers. During 2023/24, 438,716 creditor payments totalling £898.844 million were made. Of this, 87,165 totalling £399.186 million (44%) were processed from eight feeder systems which process invoices / remittances out with the eFinancials Creditors system. These feeder systems are:

1. Confirm – non-HRA property repairs
2. Firmstep – education maintenance allowance / school clothing grants
3. Spydus – library management system
4. Total – HRA building maintenance and roads
5. CorePay – payroll creditors payments
6. Key2 – vehicle maintenance and hire vehicles
7. D365 – social work care packages
8. NDR – refunds of business rates

Payment text files are generated from the feeder systems above, either as part of a scheduled automated process, or when instigated by the relevant feeder system administration staff. Similarly, Accounts Payable staff are responsible for generating the BACS payment text file from eFinancials so payment can be processed via the BACS system.

The Financial Systems Team is responsible for ensuring the accuracy of interface files uploaded to the Council's financial management system and for reconciling creditor payments made to the Council's bank account.

### 5.2 Rationale for review

The objective of this audit is to provide assurance that there are adequate controls over payments originating from creditors sub-systems.

The last full Internal Audit review of this area took place in August 2018 as part of Internal Audit AC1901 Creditor Payments when recommendations were agreed to improve written procedures; reconciliation arrangements; payment control; and limit privileged access rights. More recently Internal Audit AC2203 Financial Systems Interfaces and Reconciliations and AC2407 Creditors System carried out in November 2021 and May 2024 respectively, covered accounts payable interface and payment control processes, with recommendations agreed to restrict and monitor privileged user access (including manual adjustments to payment files); to control changes to supplier standing data affecting payments; and to enhance BACS reconciliation procedures.

This audit has been included in the agreed Internal Audit plan for 2024/25 due to the material value of payments being interfaced from sub-systems into the Creditors System and the risk of fraudulent payments if internal controls are inadequate. For example, in 2016/17, another Scottish Local Authority identified a significant fraud perpetrated by a long serving member of staff, with extensive access to several Council systems. They combined their knowledge of these systems with their unrestricted system access privileges, to insert fictitious invoices into the Creditors System for payment. This fraud perpetrated over a number of years resulted in over £1m of fraudulent payments.

### 5.3 Scope and risk level of review

This review will offer the following judgements:

- An overall **net risk** rating at the **Cluster** level.
- Individual **net risk** ratings for findings.

#### 5.3.1 Detailed scope areas

**As a risk-based review this scope is not limited by the specific areas of activity listed below. Where related and other issues / risks are identified in the undertaking of this review these will be reported, as considered appropriate by IA, within the resulting report.**

---

The specific areas to be covered by this review are:

- Written Procedures
- Segregation of Duties
- Feeder System Controls
- Receiving System Controls
- BACs Interface Controls
- Payee Data Management
- Reconciliations
- Suspense Accounts
- Monitoring Arrangements

Where individual services and risk owners are responsible for elements of the risk management framework, this review is focused on the central controls and the second line operations. As such, where we recognise many different stakeholders in the process, any recommendations made will be targeted at those centrally.

## 5.4 Methodology

This review will be undertaken through interviews with key staff involved in the process(es) under review and analysis and review of supporting data, documentation, and paperwork. To support our work, we will review relevant legislation, codes of practice, policies, procedures, and guidance.

Due to hybrid working practices, this review will primarily be undertaken remotely via electronic meetings and direct access to systems and data, with face to face contact and site visits to premises to obtain and review further records as appropriate.

## 5.5 IA outputs

The IA outputs from this review will be:

- A risk-based report with the results of the review, to be shared with the following:
  - Council Key Contacts (see 5.7 below)
  - Audit, Risk and Scrutiny Committee (final only)
  - External Audit (final only)

## 5.6 IA staff

The IA staff assigned to this review are:

- Agne McDonald, Auditor (**audit lead**)
- Andy Johnston, Audit Team Manager
- Jamie Dale, Chief Internal Auditor (**oversight only**)

## 5.7 Council key contacts

The key contacts for this review across the Council are:

- Andy MacDonald, Executive Director – Corporate Services
- Bernadette Bularan, Deputy Chief Officer – Finance (**process owner**)
- Angela Crawford, Finance Controls Manager
- Richard Burnett, Senior Accountant
- Steve Roud, Chief Officer – Digital & Technology
- Aaron Enaburekhan, Business Systems Manager

## 5.8 Delivery plan and milestones

The key delivery plan and milestones are:

---

Milestone	Planned date
Scope issued	09-Oct-24
Scope agreed	16-Oct-24
Fieldwork commences	28-Oct-24
Fieldwork completed	22-Nov-24
Draft report issued	13-Dec-24
Process owner response	17-Jan-25
Director response	24-Jan-25
Final report issued	31-Jan-25