ABERDEEN CITY COUNCIL

COMMITTEE	Audit, Risk and Scrutiny Committee
DATE	27 June 2024
EXEMPT	No
CONFIDENTIAL	No
REPORT TITLE	Internal Audit Report AC2407 – Creditors System
REPORT NUMBER	IA/AC2407
DIRECTOR	N/A
REPORT AUTHOR	Jamie Dale
TERMS OF REFERENCE	2.2

1. PURPOSE OF REPORT

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

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 the Creditors System.

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

Assessment	Outcome
Impact Assessment	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.
Privacy Impact Assessment	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 AC2407 – Creditors System

12. REPORT AUTHOR CONTACT DETAILS

Name	Jamie Dale
Title	Chief Internal Auditor
Email Address	Jamie.Dale@aberdeenshire.gov.uk
Tel	(01467) 530 988

Internal Audit

Assurance Review of the Creditors System

Status: Final
Date: 29 May 2024
Risk Level: Programme and Project

Report No: AC2407
Assurance Year: 2023/24

Net Risk Rating	Description	Assurance Assessment
Moderate	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.	**Reasonable**

Report Tracking	Planned Date	Actual Date
Scope issued	09-Nov-23	09-Nov-23
Scope agreed	24-Nov-23	23-Nov-23
Fieldwork commenced	27-Nov-23	27-Nov-23
Fieldwork completed	22-Dec-23	20-Mar-24
Draft report issued	19-Jan-24	26-Mar-24
Process owner response	09-Feb-24	22-May-24
Director response	16-Feb-24	29-May-24
Final report issued	23-Feb-24	29-May-24
AR&S Committee	27-Jun-24	

Distribution	
Document type	Assurance Report
Director	Andy MacDonald, Director – Corporate Services
Process Owner	Jonathan Belford, Chief Officer – Finance
Stakeholders	Angela Crawford, Finance Controls Manager
	Richard Burnett, Senior Accountant
	Neil Stewart, Accountant
	Steve Roud, Chief Officer – Digital & Technology
	Angela Doyle, Service Manager – Digital Service Delivery
	Ronnie McKean, Corporate Risk Lead
	Catriona Sim, Data Protection Officer
	Vikki Cuthbert, Interim Chief Officer – Governance*
***Final Only**	External Audit*
Lead auditor	Lyndsay Jarvis, Auditor

1 Introduction

1.1 Area subject to review

The Council uses eFinancials, an integrated financial system, to manage payments to suppliers of goods and services. The system is hosted by the system supplier (Advanced Business Solutions Ltd), a specialist financial software provider to the public sector, and has been in place since 1998. Internally the system is administered by the Financial Systems team who control user access and offer first line system support.

During the year to 31 March 2023, the system was used to pay approximately 196,000 invoices with a total value of approximately £951.3 million.

1.2 Rationale for review

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

This area was last audited in November 2015, report AC1606, and it was found that in general controls over the system operation were working well, the system was backed up regularly and disaster recovery testing was taking place. Recommendations were made to ensure that staff manuals are up to date and that all staff complete mandatory information security training courses. An audit on the Integrated Financial System (IFS) interfaces was carried out in November 2021, report AC2203, and it was found that in general the accuracy of financial information transferred into the IFS is well controlled, although recommendations were made to update procedures to include more information on the verification of interfaces.

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
Moderate	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.	**Reasonable**

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

Risk Level	Definition
Programme and Project	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.

2.2 Assurance assessment

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

The following governance, risk management and control measures were sufficiently robust and fit for purpose:

- **Procurement** – The Council's Financial Management System, which includes the Creditors System, has been in use since 1998. Procurement processes to renew the contract have been followed in accordance with the Council's Scheme of Governance.
- **Duplicate Payments** – The system has duplicate invoice detection and reporting functionality. In addition, Finance has engaged the service of a third-party provider who receive Council invoice files and report daily on whether or not there are any potential duplicate invoices requiring investigation.
- **Password Control** – The system requirements comply with the Council's Password Standard.
- **Payment Control** – For a sample of 15 transactions reviewed, Creditors system supplier standing data matched to details provided by suppliers and invoice data agreed to the Creditors system and BACS payment details. In addition, the BACS batch total according to the Creditors system agreed to the BACS transmission system and the Council's bank account.
- **Business Continuity and Disaster Recovery** – The Finance Business Continuity Plan was last tested in September 2022 and was reviewed in September 2023 and covers relevant procedures in the event of the loss of the Creditors system. In addition, Digital & Technology work with the Council's data centre to gain assurance over system backups for disaster recovery purposes.

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

- **Privileged Access** – Adequate control over user access rights mitigates the risk of inappropriate changes to system data, such as invoice and supplier bank details, and helps to ensure compliance with data protection legislation, by ensuring users only having access to the data that they need to fulfil their role. However privileged accounts are not subject to monitoring and are being used for administrative as well as non-administrative purposes, in breach of the Council's ICT Access Control Policy.
- **Interfaces** – Adequate written procedures are in place covering the processing of creditors interfaces from feeder sub-systems and related reconciliation arrangements. These will be considered further as part of the agreed 2024/25 agreed Internal Audit on Creditors Sub-System Payments. However, whilst for a sample of 15 transactions reviewed, BACS totals in

the Creditors system agreed to the BACS transmission system, procedures are not in place covering the BACS transmission system to Creditors system reconciliation process and this reconciliation is not recorded, risking payment discrepancies.

- **Supplier Standing Data** – The process to create and amend supplier accounts, including banking details, is mostly controlled via an automatic "Virtual Worker" process helping to ensure that information is complete, and adequate segregation of duties exists between the teams processing invoices and inputting supplier data. In addition, in certain circumstances, supplier standing data is created or amended by the Financial Systems Team (FST). However, whilst at the time of the previous audit a report on amendments to supplier data was being regularly run and monitored, this is no longer being carried out. In addition, there is presently no reconciliation of new supplier / supplier amendments to requests by Services. Also, identification and bank account evidence requirements for new payees or payee bank account changes has not been standardised for Council systems that enable payments. These matters increase the risk of payee standing data errors and fraud.
- **Invoice Processing** – A sample of 20 transactions showed four (20%) payments made over 30 days after the receipt of the invoice, making the Council potentially liable for penalties under the Late Payment of Commercial Debts (Interest) Act 1998, and risking reputational damage.

Recommendations have been made to address the above risks including enhancing training, segregating and monitoring privileged user activity, standardising requirements to verify payee identification and bank account details across Council payment systems, monitoring changes to supplier standing data, and formalising BACS transmission to Creditors system reconciliation procedures.

2.3 Severe or major issues / risks

No severe or major issues/risk were identified as part of this review.

2.4 Management response

The audit is welcomed by management, identifying various robust and appropriate processes that are standing up to scrutiny.

It is acknowledged that improvements have been identified and these will assist with enhancing the financial control environment for the paying of suppliers. Work is in progress to ensure that the actions are implemented in line with the deadlines set out.

In respect of invoice processing, the Council has been on a journey of improvement to pay more invoices within 30 days and there has been improvement in each of the last three years, recently (for 2023/24) delivering over 90% of invoices being paid within the timescale set. There remains room for improvement and to mitigate the risks described in the findings.

3 Issues / Risks, Recommendations, and Management Response

3.1 Issues / Risks, recommendations, and management response

<table>
<tr><th>Ref</th><th colspan="2">Description</th><th>Risk Rating</th><th>Minor</th></tr>
<tr><td rowspan="7">1.1</td><td colspan="4"><b>Written Procedures, Guidance and Training</b> – Comprehensive written procedures, guidance, and training, which are easily accessible by all 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.
While there are clear and comprehensive procedures available to staff both on the intranet and held within an online database managed by the FST, there is no current training in the staff portal ACC Learn, since the historic OIL portal course was removed from use. At present new users learn on the job and get guidance from the FST if requested.
Finance advised that the difficulty is because the Financial Management System encompasses many systems in one; training needs time and staff resource to develop.
However, if training is not sufficient there is a risk that staff will be unable to carry out their duties correctly or efficiently.</td></tr>
<tr><td colspan="4"><b>IA Recommended Mitigating Actions</b></td></tr>
<tr><td colspan="4">The Service should create current training resources for staff on the use of the Financial Management System.</td></tr>
<tr><td colspan="4"><b>Management Actions to Address Issues/Risks</b></td></tr>
<tr><td colspan="4"><i>Agreed. This will cover use of Creditors system and use of InfoSmart for processing invoice payments and managing invoice queries.</i></td></tr>
<tr><td><b>Risk Agreed</b></td><td><b>Person(s)</b></td><td colspan="2"><b>Due Date</b></td></tr>
<tr><td>Yes</td><td>Senior Accountant</td><td colspan="2">Jul-24</td></tr>
</table>

<table>
<tr><th>Ref</th><th>Description</th><th>Risk Rating</th><th>Moderate</th></tr>
<tr><td rowspan="2">1.2</td><td colspan="3"><b>Privileged User Access</b> – Adequate control over user access rights mitigates the risk of inappropriate changes to system data, such as invoice and supplier bank details, and helps to ensure compliance with data protection legislation, by ensuring users only having access to the data that they need to fulfil their role.
It was noted in the External Audit Annual Audit Report by KPMG reported to Audit, Risk and Scrutiny Committee in September 2022 that highly privileged or “superuser” access, required to perform user administration activities, was not always being adequately logged and monitored, creating a risk that administrator accounts could be used to inappropriately input or amend data without being recorded, and a recommendation was made to address this. The Council had responded by implementing an ICT Access Control Policy. However, the Service advised that superuser accounts were not currently monitored. In addition, it was confirmed that administrator accounts are also used for non-admin purposes e.g. Accountancy related tasks. This is a breach of the ICT Access Control Policy.</td></tr>
<tr><td colspan="3"><b>IA Recommended Mitigating Actions</b></td></tr>
</table>

Ref	Description	Risk Rating	Moderate

a) Monitoring of users including system administrators should be reviewed and where possible established to evidence compliance with the ICT Access Control Policy. This should be undertaken by officers without administrative / superuser system access and should be done with a view to reduce the risk of fraud.

b) In line with the Council's ICT Access Control Policy, administrator accounts should only be used to carry out administrative responsibilities and separate accounts should be maintained for day-to-day regular user responsibilities using a standard PoLP user account.

Management Actions to Address Issues/Risks

a) Agreed.

b) Agreed.

Risk Agreed	Person(s)	Due Date
a) Yes	Chief Officer – Finance in consultation with Chief Officer – Digital & Tech	Jul-24
b) Yes	Senior Accountant	May-24

Ref	Description	Risk Rating	Moderate

1.3

Supplier Standing Data – To mitigate the risk of fraud or error when creating and amending supplier standing data including bank account details, adequate control should be exercised over account creation and changes.

Supplier standing data is either updated via the automated "Virtual Worker" process or manually by the Financial Systems Team (FST).

Virtual Worker

The Service recently introduced the "Virtual Worker" system to increase accuracy and efficiency when inputting / amending supplier data. This deals with supplier creations where the related payment does not require a purchase order (e.g. customer refunds and grant payments) and most amendments to existing suppliers in the creditors system e.g. changes to bank details. Requestors input information to an Excel template spreadsheet available from the Finance Share/Point page, then pass to their line manager for approval.

Once submitted to AP-Development the request is then forwarded to the FinanceRPA3@aberdeencity.gov.uk inbox where it is picked up by the Virtual Worker for processing in eFinancials overnight. Forms without the required details are automatically rejected and reports detailing success or failure are received automatically daily for corrective action to be taken.

Manual Standing Data Creation / Amendment

In addition to updates processed by the Virtual Worker, manual creation / amendment of supplier standing data takes place in certain circumstances.

Where a purchase order is required to be raised for a new supplier but the supplier is absent from the purchase ordering system (PECOS), the related request must first be approved by the Commercial and Procurement Shared Service (C&PSS) via an FST99 form. The details of these suppliers, including bank details, must be provided by the supplier on the FST99 form, with an email submission from the supplier as supporting back-up. If approved, this form is sent to the Financial Systems Team (FST) in order for the supplier to be created in the creditors system.

Also, changes to bank details are occasionally processed manually by the FST directly on request. These requests are checked with the contact details held on the system and only completed once confirmation is received from the supplier via the contact made from details held on the system.

Supplier Standing Data Monitoring

However, it was noted that currently there is no system of reconciliation of changes made to standing data to Service requests, increasing the risk of inaccurate or potentially fraudulent creation or amendment of supplier standing data. This is relevant to changes by Council system administrators as well as to ensure no unauthorised changes to supplier details are made by the Virtual Worker delivery and support partner**.**

During the previous audit it was confirmed that a report was regularly run by an Accounts Payable team manager on supplier account amendments. The Service advised that this is no longer being carried out. Reinstating the amendments report and introducing a system of reconciliation would give assurance that any inappropriate or unauthorised changes are detected, reducing the possibility of fraud. Ideally this should be carried out by someone without access to make amendments.

Supplier Standing Data Evidence

In addition, it was noted on discussion with Finance that at present, regardless of the standing data update process, evidence required to prove identification of the payee and their bank details has not been standardised, meaning the identity of any individual providing new bank details is not being confirmed nor are the proposed bank details to be used, increasing the risk of fraud.

IA Recommended Mitigating Actions

a) Finance should standardise payee identification and bank account evidence requirements for the purposes of making payments generally and establish a verification process for ensuring this evidence is in place before the related Council system account can be used to make payments to the respective payee. This should be carried out for all systems that can be used to make payments with a view to reducing the risk of fraud. Any exceptional payments in the absence of adequate payee identification and bank statement evidence should be risk assessed, clearly defined and approved by the Chief Officer – Finance.

b) Finance should carry out regular monitoring of supplier standing data amendments. As well as covering superuser changes this should include a reconciliation of changes / new supplier standing data processed by the Virtual Worker as compared to related requests by Services.

Management Actions to Address Issues/Risks

a) Standardise process to include collation of Bank Statement (could accept screenshot of internet banking if no access to printer or unable to attend) This would be approved by the service if insufficient backup sent in and all necessary checks had been made.

b) Monthly checks to be implemented by Creditors team from report of all amends and a 10% check made, verified and returned to systems team by email with a note of items checked for filing by systems team as a means of record of the check being done. A reconciliation of *standing data changes in the creditors system processed by the Virtual Worker to the related email submission of these changes will also be undertaken.*

Risk Agreed	Person(s)	Due Date
a) Yes	a) Finance Controls Manager	Dec-24
b) Yes	b) Finance Controls Manager	Jul-24

Ref	Description	Risk Rating	Moderate
1.4			

Interfaces – 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.

Adequate written procedures are in place covering the processing of creditors interfaces from feeder sub-systems and related reconciliation arrangements. These will be considered further as part of the agreed 2024/25 agreed Internal Audit on Creditors Sub-System Payments.

However, whilst for a sample of 15 transactions reviewed, BACS totals in the Creditors system agreed to the BACS transmission system, procedures are not in place covering the BACS transmission system to Creditors system reconciliation process and this reconciliation is not recorded, risking payment discrepancies.

IA Recommended Mitigating Actions

The Service should establish written procedures for the Creditors System to BACS transmission system payment file transfer reconciliation and evidence of this reconciliation should be recorded.

Management Actions to Address Issues/Risks

Agree a procedure and record a check that the reconciliation has been done on a daily basis

Risk Agreed	Person(s)	Due Date
Yes	Finance Controls Manager	Jul-24

Ref	Description	Risk Rating	Moderate
1.5			

Invoices: Late Payment – The Late Payment of Commercial Debts (Interest) Act 1998 requires public authority's such as the Council to pay their debts within 30 days. If this is not achieved a supplier may seek compensation as a result of costs incurred recovering the debt and statutory interest may be applied. It is important that invoices are processed and paid timeously in order to avoid late penalties / interest, reputational damage and preserve good working relationships with suppliers.

A sample of 20 transactions was selected at random from a transactions report drawn from the Creditors system and reviewed. In all cases all required information was present and the invoice once matched and authorised was paid promptly. However in four cases the payments were not made within 30 days of receipt of the invoice.

Ref	Description	Risk Rating	Moderate

For sample 1, which took 135 days to resolve, the invoice could not be automatically matched to the purchase order and the originating Service (E&CS) did not amend the order as required. When the supplier put a stop on the Council's account the Accounts Payable team amended the invoice category manually to remove the need for purchase order matching so that it could be processed; this was authorised by the Finance Controls Manager.

For sample 3, which took 133 days to resolve, the invoice could not be automatically matched to the purchase order and the employee within the originating Service (CH&I) who had placed the order had left their role so was not available to amend the order. The responsibility was not taken on by another member of staff until the supplier put a stop on the Council's account.

For sample 18, which took 46 days to resolve, the invoice was not imported into the system until after its due date. The Service responsible (E&CS) advised that the PO had been raised retrospectively after a booking had been made without a PO.

For sample 19, which took 32 days to resolve, no purchase order was available for automatic matching and it took 24 days for the originating Service (E&CS) to identify an employee who could authorise the payment.

Finance already remind users at least monthly of invoices which either require authorisation in the InfoSmart system or require goods / services to be receipted in PECOS to enable payment. However, the above examples indicate there is still an issue with Services delaying payment.

Late payments can potentially make the Council liable for penalties under the Late Payment of Commercial Debts (Interest) Act 1998, and risk reputational damage and the withdrawal of supply of goods or services. Finance advised that when issues are identified they work with Services to resolve them, offering one-to-one coaching where relevant. However, a more proactive approach, such as comprehensive and accessible training and regular communication on this issue would help mitigate problems arising in the first place. A recommendation to improve training resources is made in 1.1.

IA Recommended Mitigating Actions

Finance should establish a system of escalation for overdue invoices with a training requirement for staff where appropriate.

Management Actions to Address Issues/Risks

1.1 refers to training guides – remind users of the availability of these guides. Build on our reporting that we have just now by checking report with previous month and escalate to Chief Officer any items that have not been addressed from previous month

Risk Agreed	Person(s)	Due Date
Yes	Finance Controls Manager	Jul-24

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
Corporate	This issue / risk level impacts the Council as a whole. Mitigating actions should be taken at the Senior Leadership level.
Function	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.
Cluster	This issue / risk level impacts a particular Service or Cluster. Mitigating actions should be implemented by the responsible Chief Officer.
Programme and Project	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
Minor	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.	**Substantial**
Moderate	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.	**Reasonable**
Major	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.	**Limited**
Severe	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.	**Minimal**

Individual issue / risk	Definitions
Minor	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.
Moderate	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.
Major	The absence of, or failure to comply with, an appropriate internal control, such as those described in the Council's Scheme of Governance. This could result in, for example, a material financial loss, a breach of legislative requirements or reputational damage to the Council. Action should be taken within three months.
Severe	This is an issue / risk that is likely to 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. Examples include a material recurring breach of legislative requirements or actions that will likely result in a material financial loss or significant reputational damage to the Council. Action is considered imperative to ensure that the Council is not exposed to severe risks and should be taken immediately.

5 Appendix 2 – Assurance Scope and Terms of Reference

5.1 Area subject to review

The Council uses eFinancials, an integrated financial system, to manage payments to suppliers of goods and services. The system is hosted by the system supplier, a specialist financial software provider to the public sector, and has been in place since 1998. Internally the system is administered by the Financial Systems team who control user access and offer first line system support.

During the year to 31 March 2023, the system was used to pay approximately 196,000 invoices with a total value of approximately £951.3 million.

5.2 Rationale for review

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

This area was last audited in November 2015, report AC1606, and it was found that in general controls over the system operation were working well, the system was backed up regularly and disaster recovery testing was taking place. Recommendations were made to ensure that staff manuals are up to date and that all staff complete mandatory information security training courses. An audit on the Integrated Financial System (IFS) interfaces was carried out in November 2021, report AC2203, and it was found that in general the accuracy of financial information transferred into the IFS is well controlled, although recommendations were made to update procedures to include more information on the verification of interfaces.

5.3 Scope and risk level of review

This review will offer the following judgements:

- An overall **net risk** rating at the **Programme and Project** 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:

- Policies and Procedures
- System Access
- Procurement and Contract Monitoring
- System Maintenance
- System Interfaces
- Supplier Data
- Invoice Processing and Payment
- BACS payment process
- Reporting and Reconciliations
- Business Continuity and Disaster Recovery

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, guidance.

Due to hybrid working across the Council, this review will be undertaken primarily remotely.

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 1.7 below)
  - Audit Committee (final only)
  - External Audit (final only)

5.6 IA staff

The IA staff assigned to this review are:

- Lyndsay Jarvis, **(audit lead)**
- Andrew 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:

- Steven Whyte, Director – Resources
- Jonathan Belford, Chief Officer – Finance (**process owner**)
- Craig Innes, Chief Officer – Commercial & Procurement Services
- Steve Roud, Chief Officer – Digital & Technology

5.8 Delivery plan and milestones

The key delivery plan and milestones are:

Milestone	Planned date
Scope issued	09-Nov-23
Scope agreed	24-Nov-23
Fieldwork commences	27-Nov-23
Fieldwork completed	22-Dec-23
Draft report issued	19-Jan-24
Process owner response	09-Feb-24
Director response	16-Feb-24
Final report issued	23-Feb-24