ITEM No …4……..

REPORT TO: **SCRUTINY COMMITTEE – 5 FEBRUARY 2025**

REPORT ON: **INTERNAL AUDIT REPORTS**

REPORT BY: **CHIEF INTERNAL AUDITOR**

REPORT NO: **35-2025**

1.0 PURPOSE OF REPORT

To submit to Members of the Scrutiny Committee a summary of the Internal Audit Reports finalised since the last Scrutiny Committee.

2.0 RECOMMENDATIONS

Members of the Committee are asked to note the information contained within this report.

3.0 FINANCIAL IMPLICATIONS

None

4.0 MAIN TEXT

4.1. The day-to-day activity of the Internal Audit Service is primarily driven by the reviews included within the Internal Audit Plan. On completion of a specific review, a report which details the audit findings and recommendations is prepared and issued to management for a formal response and submission of management's proposed action plan to take the recommendations forward. Any follow-up work subsequently undertaken will examine the implementation of the action plan submitted by management.

4.2. Executive Summaries for the reviews which have been finalised in terms of paragraph 4.1 above since the last Scrutiny meeting are provided at Appendix A. The full reports are available to Elected Members on request. Reporting in Appendix A covers:

Audit	**Assurance level**
Corporate Debt Recovery	Limited Assurance
User Access Management	Limited Assurance

4.3. Internal audit recommendations are now being categorised as either relating to the design of the control system (Design) or compliance with the operation of the controls (Operational). A comment on this is now included in each report.

5.0 POLICY IMPLICATIONS

This report has been subject to the Pre-IIA Screening Tool and does not make any recommendations for change to strategy, policy, procedures, services, or funding and so has not been subject to an Integrated Impact Assessment. An appropriate senior manager has reviewed and agreed with this assessment.

6.0 CONSULTATIONS

The Council Leadership Team have been consulted in the preparation of this report.

7.0 BACKGROUND PAPERS

None.

CATHIE WYLLIE, CHIEF INTERNAL AUDITOR **13 JANUARY 2025**

(i) INTERNAL AUDIT REPORT 2023/21

Client	**Corporate Services – Corporate Finance**
Subject	**Corporate Debt Recovery**

Executive Summary

Conclusion

Limited Assurance
There is limited formal definition and documentation of individual responsibilities in the Council's Sales Ledger debt recovery processes, and the resulting variation in approach means that management cannot easily evidence that processes are working efficiently and adequately mitigating risk. Elements of authorisation and approval are not operating as designed.

Background

Individuals and organisations can become debtors of the Council for a variety of reasons: through liability for council tax or rates, as a council tenant, statutory charges and fees, or as the recipient of services charged by invoice.

Where services are charged by invoice, these are raised across Services through the centrally administered sales ledger system. The resulting debts are managed by the Corporate Collections Team, which seeks to ensure that outstanding debts are monitored and pursued, and in the event of non-payment, are referred for enforcement or written off in accordance with the Council's policies. The team also performs this function for external bodies and partners including Leisure & Culture Dundee and Tayside Pension Fund.

Outstanding sales ledger debt across all Services and Council bodies is typically £15-18m at any point in time, with millions of pounds received in payment each month.

Scope

Review of the Council's Sales Ledger debt management and debt recovery arrangements.

The review considered the risks arising from Sales ledger income processes but did not examine processes which apply to income streams for Council Tax, Business Rates and Housing Rents.

Objectives

		Action Priority			
		C	H	M	L
Processes are in place to ensure that outstanding sales ledger debt is pursued on a timely basis, in a manner which maximises the likelihood that the debt is paid	**Limited Assurance**	-	1	1	-
Levels of outstanding and aged debt, and individual debtor balances are regularly monitored	**Limited Assurance**	-	1	-	-
Policies are in place which establish the circumstances in which aged debt is referred for legal action or write-off, and these are consistently applied	**Limited Assurance**	-	-	1	-
Debt recovery performance is appropriately monitored and reported to senior management	**Substantial Assurance**	-	-	-	-
TOTAL		-	2	2	-

Nature of Recommendations

Two (one high, one medium) of the recommendations relate to the design of controls, and two (one high, one medium) to the operation of existing controls. This suggests that the control framework itself requires revision to adequately address the risks identified.

Key Findings

We identified areas of good practice:

- Management information relating to debt recovery is consistently prepared in a standard format, providing senior management with an overview of volumes and value of outstanding debt, and clear indications as to whether the position is improving or deteriorating.

We have identified the following areas for improvement:

- Key policies and procedures should be documented, as existing documentation does not explicitly address some of the actions required in management of an outstanding debt or matters such as the delegation of responsibilities within the Collections Team.
- The guidance available to officers does not address more complex recovery situations. Guidance sets out a relatively straightforward pathway in which individuals are chased for payment and that payment is either made or the matter is referred for legal action. In practice, some recoveries involve establishing payment arrangements or management of disputes, however there is no consistent approach to how these are administered and managed.

- Adherence to timelines for the pursuit of debts is inconsistent, likely as a consequence of individual decisions as to which debts to pursue as a part of workload management. The lack of a defined approach means that it is difficult to establish the effectiveness and efficiency of the decisions made in the course of pursuing individual debts.
- Inconsistency between established practice and template documentation creates uncertainty as to whether authorisation requirements had been applied. As a consequence of the lack of guidance, decisions to refer a debt for write off are taken on different bases by different individuals.

Impact on risk register

The Corporate and Service risk registers included, at time of audit, the following risks:

- DCC001 Financial Sustainability (inherent risk 5x4, residual risk 5x4)
- DCC013, CSCF011 Fraud & Corruption (inherent risk 4x5, residual risk 4x3)
- CSCF008 Compliance (inherent risk 5x5, residual risk 5x3)
- CSCF010 Finance – Management (inherent risk 5x5, residual risk 5x4)

The process of Corporate Debt Recovery is intended to mitigate the risk that the Council does not receive money which it is owed. Within the scope of this review, the financial value at risk can be quantified as being approximately £750,000 written off in 2023/24, which impacts upon the Council's financial sustainability. Monitoring, oversight, and scrutiny arrangements over the process contribute to the mitigation of Fraud & Corruption and Financial Management risks.

The internal controls identified against these risks in the Corporate and Service risk registers consist of:

- Job related Training and Awareness
- Management Supervision, authorisation, and checking process
- Segregation of duties
- General monitoring and reporting controls

We have identified areas for improvement in relation to the guidance, policy, and process documentation that underpins supervision and authorisation processes. We have determined that authorisation processes in relation to write off of debt are not operating effectively, and that as a consequence there is a gap in segregation of duties.

Risk owners should consider whether risks remain accurately scored in the light of the findings of this review.

(ii) INTERNAL AUDIT REPORT 2023/29

Client	**Corporate Services – Corporate Finance**
Subject	**User Access Management**

Executive Summary

Conclusion

Limited Assurance
There is a need to develop and maintain formal procedures for both system administration and general users of the Civica systems. We found there to be no documented procedures covering areas such as joiners, movers and leavers as well as user access reviews and periodic management and maintenance tasks. There are no user role matrices for Civica Financials or Purchasing which sets out the basis on which access will be granted to users. At present, access is granted by copying the access profile of another user. Processes in relation to user access reviews need improvement. Whilst there is a six-monthly check of active Civica Financials privileged accounts, the current process for reviewing general user accounts needs to be updated. The current process only checks 24 of over 900 registered users each year which is not sufficient. Our review of Civica Purchasing accounts identified weaknesses in the review process. A large number of accounts were active despite not being used in over one year. There is no monitoring of Civica user activity. Whilst audit logs are being created, they are only reviewed in response to a specific request. There is also no monitoring of privileged user activity to confirm that they have only been used for valid purposes.

Background

User access management is recognised as one of the key information security controls for the Council in protecting the confidentiality, integrity and availability of information. User access management is used to enable and / or restrict access to individuals to read or amend information.

The Council operates the Civica Financials system. This is a business-critical tool which supports the production of financial and management accounts as well as the generation of sales invoices and processing of purchase invoices. The nature of the application means that it is essential that access management ensures only authorised users have access and that segregation of duties is achieved when granting access privileges.

Scope

Our review examined the user account and access management controls in place within the Council that ensure the confidentiality, integrity and availability of the Civica Financials system data. The review also considered the adequacy of user access controls to ensure effective segregation of duties.

Objectives

		Action Priority			
		C	**H**	**M**	**L**
There are adequate system administration and user procedures in place.	**Substantial Assurance**	**-**	**-**	**2**	**-**
There is effective user account management which ensures only authorised users have access.	**Substantial Assurance**	**-**	**-**	**1**	**-**
User access levels are appropriate and ensure adequate segregation of duties in relation to the administration and operation of the system.	**Limited Assurance**	**-**	**-**	**1**	**-**
There are appropriate audit facilities within the system to allow effective and regular monitoring of the application.	**Limited Assurance**	**-**	**1**	**-**	**-**
TOTAL		**-**	**1**	**4**	**-**

Nature of Recommendations

All of the recommendations (1 High, 4 Medium) relate to the design of controls as opposed to the operation of existing controls. This suggests that the control framework itself requires revision to adequately address the risks identified.

Key Findings

We have identified the following areas for improvement:

- There is a need to develop documented procedures for the system administration and day-to-day use of Civica. Many current processes were not documented and there was a lack of consistency in process between the respective Civica Financials and Purchasing administration teams.
- There are no role matrices which set out the access requirements for user roles for Civica.
- There is no documentation setting out who has authority to approve and submit Civica Financials joiners, movers, and leavers requests.
- User access reviews need improvement. There are no reviews for Civica Financials and the current process for Civica Purchasing could be improved.
- There is no monitoring of user access and user activity within Civica.

Impact on risk register

The (Service) risk register included, at time of audit, the following risks:

- CSCS003 IT / Systems (inherent 5 x 3, current 4 x 2)
- CSCS010 Failure to remove systems access following an officer status change (inherent 5 x 4, current 5 x 3)

- CSIT005 Failure to protect sensitive data (inherent 4 x 4, current 3 x 3)
- CSIT008 Overreliance on key individuals with key knowledge or experience (inherent 3 x 4, current 3 x 3)
- CSIT009 Failure to control IT user access (inherent 4 x 5, current 3 x 2)
- CSIT016 Failure to remove systems access following an officer status change (inherent 5 x 4, current 5 x 3)

Our review has identified findings against the following risks:

- CSCS010 Failure to remove systems access following an officer status change (inherent 5 x 4, current 5 x 3)
- CSIT009 Failure to control IT user access (inherent 4 x 5, current 3 x 2)
- CSIT016 Failure to remove systems access following an officer status change (inherent 5 x 4, current 5 x 3)
- In light of our findings and, in particular, the inability to provide user access information for Civica Purchasing the current risk level for CSIT009 appears low. Management should reconsider this risk rating when reflecting on the response to this report.

Definitions of Levels of Assurance

Comprehensive Assurance	The system of controls is essentially sound and supports the achievement of objectives and management of risk. Controls are consistently applied. Some improvement in relatively minor areas may be identified.
Substantial Assurance	Systems of control are generally sound, however there are instances in which controls can be strengthened, or where controls have not been effectively applied giving rise to increased risk.
Limited Assurance	Some satisfactory elements of control are present; however, weaknesses exist in the system of control, and / or their application, which give rise to significant risk.
No Assurance	Minimal or no satisfactory elements of control are present. Major weaknesses or gaps exist in the system of control, and / or the implementation of established controls, resulting in areas of unmanaged risk.

Definitions of Action Priorities

Critical	**Very High-risk exposure to potentially major negative impact** on resources, security, records, compliance, or reputation from absence of or failure of a fundamental control. Immediate attention is required.
High	**High risk exposure to potentially significant negative impact** on resources, security, records, compliance, or reputation from absence of or non-compliance with a key control. Prompt attention is required.
Medium	**Moderate risk exposure to potentially medium negative impact** on resources, security, records, compliance or reputation from absence or non-compliance with an important supporting control, or isolated non-compliance with a key control. Attention is required within a reasonable timescale.
Low	**Low risk exposure to potentially minor negative impact** on resources, security, records, compliance, or reputation from absence of or non-compliance with a lower-level control**, or areas without risk exposure but which are inefficient, or inconsistent with best practice.** Attention is required within a reasonable timescale.