ITEM No …8……..

REPORT TO: **SCRUTINY COMMITTEE - 25 JUNE 2025**

REPORT ON: **INTERNAL AUDIT REPORTS**

REPORT BY: **CHIEF INTERNAL AUDITOR**

REPORT NO: **178-2025**

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**
User Access Management – Northgate Citizens Access	Substantial Assurance
Microsoft Office 365	Limited Assurance
Risk Management	Substantial Assurance
Insurance	Substantial Assurance
Payroll – Changes in Circumstances	Substantial Assurance
Civica CX – Rent Accounting Module	Substantial Assurance

4.3. Internal audit recommendations are categorised as either relating to the design of the control system (Design) or compliance with the operation of the controls (Operational).

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 **4 JUNE 2025**

(i) INTERNAL AUDIT REPORT 2024/06

Client	**Corporate Services – Customer Services and IT**
Subject	**User Access Management – Northgate Citizens Access**

Executive Summary

Conclusion

Substantial Assurance
Overall, our audit work identified that user access management of Citizens Access - Revenues (CA-R) was subject to adequate levels of control. The system has been relatively recently implemented and there has been low turnover of users since early 2024. We have set out, below, areas where controls could be enhanced. There are comprehensive manuals provided by Northgate which cover the vast majority of user and system administration actions. There may be merit in extending this documentation to include a formally documented procedure for new starts, movers and leavers. A review of Revenues & Benefits staff user access should be performed. A wider review of systems user access was performed in autumn 2024, but a review of CA-R access was excluded from this due to the system only being live for six months. In addition, there should be more frequent review of accounts with privileged access in line with leading practice. The Council would benefit from gaining clarity on responsibilities for monitoring of the system for performance as well as anomalous internal and external activity. This review should be led by the Systems Team. Once clarification is obtained, the Council should receive assurances and reports from Northgate to confirm that they are performing this monitoring.

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 has introduced a Citizens Access portal within the Northgate system. This provides citizens with the ability to view and update certain information such as updating address or household information. It is vital that there are appropriate controls in place to ensure that user access is validated and there are secure mechanisms for updating information.

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 Citizens Access data. The review also considered the adequacy of user access controls.

Objectives

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

Nature of Recommendations

All of the three recommendations made relate to issues identified with the design of existing controls and represent instances in which the control framework requires revision to adequately address risks.

Key Findings

We have identified the following areas for improvement:

- There is no documentation setting out who has authority to approve and submit Northgate joiners, movers, and leavers requests.
- User access reviews need improvement. The current process which is followed for the reviews of the Northgate system could be improved.
- There is a need for the Systems Team to confirm that there is sufficient monitoring performed by Northgate of the internal and external access to the CA-R system.

Impact on Risk Register

The Customer Services and Council Advice Services (CSCS) as well as the ICT risk registers include the following risks relevant to this review:

- CSCS002 Information/GDPR/Confidentiality (inherent 5 x 5, current 5 x 3)
- CSCS003 IT / Systems (inherent 5 x 3, current 4 x 2)
- CSCS008 Fraud & Corruption (inherent 5 x 5, current 5 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)
- CSCF028 Data Protection/Information Governance (inherent 5 x 5, current 5 x 3)

Our review has identified findings against the following risks:

- CSIT009 Failure to control IT user access (inherent 4 x 5, current 3 x 2)
- In light of our findings the current risk level for the above risk appears appropriate.

(ii) INTERNAL AUDIT REPORT 2023/28

Client	**Corporate Services – Customer Services and IT**
Subject	**Microsoft 365**

Executive Summary

Conclusion

Limited Assurance

Our review found that the Council has scope to improve processes in place to manage access to and invoke security controls over Microsoft 365. We did note that Multi-Factor Authentication was in place for access to Microsoft 365.

User access is driven by Active Directory. This has meant that issues managing Active Directory access have been mirrored in Microsoft 365 access. For example, we found discrepancies in account access as a result of:

- lack of documentation on the purpose of generic accounts and their regular review.
- lack of assurance from HR to confirm that the biannual user review process has been undertaken and changes processed.
- issues in automated elements of the leavers processes not being identified and addressed. Due to this, we identified an active administrative account for someone who has left the Council.

The Council would benefit from invoking more stringent controls over access management to ensure only those authorised to use Microsoft 365 resources have access to do so.

Additionally, policies and procedures do not set out requirements for access management and application use of Microsoft 365 products. As such, there is limited guidance in place as to how Microsoft 365 applications may be used, and configuration of these applications is generally unrestricted.

In addition, the Council has implemented some data loss prevention rules however these could be improved upon to reflect the risks of the use of cloud applications on personal devices.

Background

As part of the response to the Covid-19 pandemic, the Council, like many organisations, migrated to using the Microsoft 365 platform. This provided a cloud-based service for office productivity tools such as Word, Excel and Outlook as well as access to Teams, a key tool that facilitated internal and external communication.

One of the benefits of the Microsoft 365 platform is that it has the capability to be accessed from any device – personal and corporate – unless it is configured to prevent this. A key element of successful management of Microsoft 365 is ensuring that it is configured to maximise operational effectiveness and efficiency whilst minimising cyber and data security risk. For example, it is recommended to have multi-factor authentication enabled to reduce the risk of Council user accounts being hacked.

Scope

The review assessed the adequacy of access management controls over the Microsoft 365 environment. Our review also considered the adequacy of security configuration which minimises risk to data held within Microsoft 365. This included how the Council has configured the service to prevent access to data from devices where this is no longer required.

Objectives

		Action Priority			
		C	H	M	L
There are effective user account management processes to ensure that only authorised users have access to Microsoft 365 resources.	**Limited Assurance**	-	2	-	-
There are effective processes to ensure that users only have access to the data that is relevant to their role.	**Limited Assurance**	-	3	-	-
Multi-factor authentication has been implemented to strengthen user account security.	**Comprehensive Assurance**	-	-	-	-
There are adequate policies covering the access management and use of Microsoft 365	**Limited Assurance**	-	1	-	-
Tools are in place and configured for data loss prevention, including remote wiping of data from any mobile and portable devices.	**Limited Assurance**	-	1	-	-
TOTAL		-	7	-	-

Nature of Recommendations

Six (all high) of the seven recommendations made relate to issues identified with the design of existing controls and represent instances in which the control framework requires revision to adequately address risks. The remaining recommendation relates to the operation of the existing controls.

Key Findings

We have identified the following areas for improvement:

- Access management controls do not include regular review of generic and administrative accounts. This has resulted in generic accounts which cannot be fully explained and one administrative account found to be active for a user who had left the Council.

- Our audit work identified that the automated process within IT to assign disablement and expiration dates to the accounts of individuals departing the organisation was not working. This had not been identified by management.

- Applications such as Microsoft Teams are unrestricted in their configuration. There is limited guidance in place setting out what data may be stored in a given application and who may be granted access to this.

- Policies and procedures do not set out requirements for and approaches to access management and the use of Microsoft 365 within the Council.

- Some Data Loss Prevention (DLP) rules have been implemented however these could be enhanced to reflect the risks of users accessing Microsoft 365 applications on their personal devices. No testing of Data Loss Prevention approaches and configuration is undertaken.

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 all of the above risks, with the exception of CSIT 008 (Overreliance on key individuals with key knowledge or experience).

In light of the findings in this report, particularly those around privileged access accounts, lack of controls over Microsoft Teams access and weaknesses in relation to leavers, we recommend that the IT team reviews all of the current risk ratings for the relevant risks above.

(iii) INTERNAL AUDIT REPORT 2024/04

Client	**Corporate**
Subject	**Risk Management**

Executive Summary

Conclusion

Substantial Assurance

This review assessed the adequacy and effectiveness of the Council's risk management framework, with particular focus on risk identification, ownership, scoring and prioritisation, mitigation, monitoring, and reporting.

We found that the Council has established a structured approach to risk management, underpinned by a Risk Management Policy and Strategy that sets out roles, responsibilities, and the process for assessing and managing risks. The use of a 5x5 risk scoring matrix and supporting procedural guidance reflects standard practice and provides a consistent method for assessing risk severity and likelihood.

Risks are regularly discussed at both operational and strategic levels through established governance forums, including the Risk and Assurance Board (RaAB) and the Council Leadership Team (CLT). These forums play a central role in overseeing the Corporate Risk Register (CRR) and ensuring ongoing scrutiny and challenge of risk positions.

However, we have highlighted several areas for improvement, including inconsistencies in the application of risk scoring, missing mitigating actions, and the absence of target risk scores across sampled risks. Additionally, while review frequencies were generally set, there were instances where reviews were overdue or lacked sufficient commentary to justify the current position of the risk.

Background

The Council's Risk Management Policy and Strategy document was reviewed by the City Governance Committee on 21 August 2023, and prior to this at five-yearly intervals in 2018 and 2013. As part of the most recent review, the Council's risk appetite was updated, and the remit of the Risk and Assurance Board (RaAB) was appended to the strategy/policy document.

This Board was created in 2022 as a replacement to the Risk Management Working Group and is responsible for providing assurance and recommendations in relation to: the Risk Management arrangements, the Council's internal audit provision, and any updates and/or changes in legislation and regulation. The RaAB meets every two months and reports to the Council's Leadership Team (CLT).

The Council maintains a Corporate Risk Register which is subject to regular review during the year by the CLT and the RaAB. The Corporate Risk Register contains the Council's strategic risks, and Service Area Risk Registers comprise operational risks relevant to each area which are maintained using the Risk Module within Pentana software. Comprehensive procedures are in place to support the implementation of the Risk Management Policy and Strategy, including instructions on using the Pentana Risk Module to record the management of the Council's strategic and operational risks.

Each Service Area is responsible for managing its own risks and ensuring information held on Pentana is up to date and accurate. The Corporate Risk Management Co-ordinator post has been vacant since September 2023 when the post holder retired. In the meantime, the Acting Senior Manager, Internal Audit has been responsible for overseeing the co-ordination of the Council's approach to risk management.

Scope

The audit was a high-level review of the Council's risk management framework to ensure that there are appropriate arrangements in place to assist in ensuring risks to the achievement of the Council's objectives are identified and effectively managed with appropriate actions put in place to mitigate them.

Objectives

		Action Priority			
		C	H	M	L
Control Objective One: An appropriate Risk Management strategy/policy exists which clearly sets out roles and responsibilities, the Council's approach and appetite for risk, and is supported by comprehensive procedures.	**Substantial Assurance**	-	-	2	1
Control Objective Two: Effective arrangements for identifying risks are in place which include the correlation between risk management and the business planning process.	**Limited Assurance**	-	-	1	-
Control Objective Three: Risks are recorded within appropriate risk registers at strategic and operational levels and are assigned risk owners.	**Limited Assurance**	-	-	2	-
Control Objective Four: An appropriate methodology exists for scoring risks and for their prioritisation.	**Substantial Assurance**	-	-	-	1
Control Objective Five: Effective risk mitigation/treatments are put in place for each risk with risks and their related mitigating actions being subject to regular monitoring and review. Arrangements are in place for escalating risks, if necessary.	**Limited Assurance**	-	-	1	1
Control Objective Six: Effective risk mitigation/treatments are put in place for each risk with risks and their	**Comprehensive Assurance**	-	-	-	-

related mitigating actions being subject to regular monitoring and review. Arrangements are in place for escalating risks, if necessary.					
TOTAL		**-**	**-**	**6**	**3**

Nature of Recommendations

Nine recommendations were raised in total. Seven relate to issues identified with the design of existing controls and represent instances in which the control framework requires revision to adequately address risks. Two relate to the operation of controls and are primarily about ensuring consistency of application of the controls.

Key Findings

We identified the following areas of good practice:

- Risk management is actively monitored through established governance arrangements, including the Risk and Assurance Board, which meets every two months and includes risk as a standing agenda item.

- The Council Leadership Team (CLT) plays an active role in reviewing and approving updates to the Corporate Risk Register (CRR). Papers submitted to CLT show ongoing consideration of risk positions, scoring adjustments, and control effectiveness.

- Risk registers show historical changes in risk scores, enabling clear tracking of whether risks are increasing or being successfully mitigated over time.

We have identified the following areas for improvement:

- Updating the version of the Risk Management Policy and Strategy available on internal platforms such as Pentana to ensure staff are working with the current version.

- Revising and enhancing the Risk Management Procedures to provide more details and practical guidance to staff.

- Developing and formalising a risk appetite for operational risks to help ensure that risk decisions are informed and consistent at all levels of the organisation. Reviewing the risk appetite statement is at least annually and updating it whenever significant changes occur.

- Reviewing the current identification process to ensure it is actively capturing emerging risks across all service areas.

- Reviewing all risk registers to ensure that every risk has clearly assigned owners, including “Assigned To” and “Managed By,” and that these roles are different, in line with current guidance.

- Implementing a recurring reminder or review mechanism to verify accuracy, particularly when staff leave or change roles.

- Conducting a comprehensive review of risks recorded in Pentana across all levels.

- Providing targeted training sessions for staff involved in risk assessment to ensure a consistent understanding and application of the risk scoring and prioritisation methodology.

- Providing refresher training for key staff on updated procedures, use of Pentana, and interpreting/applying risk appetite in their decision-making.

- Ensuring all risks include a clear target risk score and a target date for achievement. All risks with a medium or high residual score should have clearly defined SMART mitigating actions linked in Pentana.

- Introducing a formal mechanism for evaluating the effectiveness of internal controls during each review cycle. Ensure that any changes to risk scores are accompanied by sufficient narrative commentary.

Impact on Risk Register

This review is relevant to all risks included within the Council's risk registers.

(iv) INTERNAL AUDIT REPORT 2024/16

Client	**Corporate**
Subject	**Insurance**

Executive Summary

Conclusion

Substantial Assurance

This review assessed the adequacy and effectiveness of the Council's insurance claims handling process, with particular focus on claims recording, processing, monitoring and reporting.

We found that the Council has established a structured approach to insurance claims handling, underpinned by the Claims Handling Agreements with Travelers and Zurich Municipal, alongside several individual procedure documents which covers handling Public Liability, Motor and Property claims. The controls in place to ensure that claims are processed in an efficient and effective manner are generally operating well.

Staff members in the Insurance and Loss Control team have received sufficient training to ensure their knowledge of Insurance and claims handling is kept up to date. Our sample testing confirmed that claims on Claim Control are being filled out completely, with all relevant records and documentation stored on the system.

However, we have noted the absence of a single overarching Claims Management Handbook which consolidates all key processes, outlines roles and responsibilities, clarifies authorisation limits and sets out expectations for quarterly file reviews.

We obtained a copy of all insurance claims processed by Council over the past 12 months and identified that 3.5% Public Liability claims, 4.8% Property claims and 32.3% Motor claims remain open. The average time taken to settle closed claims was 73 days for Public Liability, 32 days for Property, and 81 days for Motor claims. We acknowledge that there are currently no defined timescales for resolving claims, largely due to third-party involvement and internal resource constraints.

The quarterly file reviews process could also be further strengthened and formally documented in a Claims Management Handbook to help ensure all claims are actively monitored and addressed.

Background

As part of its responsibilities, the Council's Insurance and Loss Control Team is responsible for ensuring that the Council's assets are adequately and effectively insured. This is achieved by having an insurance programme in place with a number of external insurance companies and a self-insured programme. The Team is also responsible for dealing with insurance claims made against the Council and pursuing recovery of costs against third parties. e.g. those who have caused damage to Council property.

The contract for the provision of insurance cover to the Council was put out to tender in 2023, with insurance companies invited to bid for three lots related to cover for the following areas – Property, Liabilities and Motor. Following this competitive tendering exercise, the largest lots

were awarded to Travelers and Zurich Municipal with effect from 31 December 2023. In addition, the Council has insurance contracts in place with AIG UK, RSA and Zurich Engineering to cover school journeys/travel, marine insurance and engineering inspections.

Claims handling agreements are in place with each of the insurance companies which set out who is responsible for dealing with any claims which are received (i.e. the Council or the relevant insurance company) depending on the type of insurance cover and the value of the claim. For example, all personal injury claims are processed by the insurers. However, motor insurance claims are handled in-house by the Council.

The Insurance and Loss Control Team uses Claim Control (Alphatec's web-hosted application insurance management system) to process claims including recording and analysing incidents and assessing claims made against the Council. The system is also used to assist in the prompt settlement/payment of claims and for management information and reporting purposes.

The Council's Insurance and Loss Control Team maintains Stop Loss reports which set out details of the claims which have been handled by the Team, including the date of the incident, its cause and description, the claimants' name, vehicle registration number (for motor claims), the settlement date, the total reserve amount, and the paid (settled) amount. These reports are submitted to the insurers on a quarterly basis.

Scope

The audit has focused on the controls in place over insurance claims handling to ensure that claims are processed in an efficient and effective manner in accordance with claims handling agreements and the requirements of the relevant policy. This review has been limited to the review of claims processed by the Council's in-house Team and has only included claims processed on behalf of the Council. Claims processed by the in-house Team on behalf of any external agencies have, therefore, been excluded from this review.

Objectives

		Action Priority			
		C	H	M	L
Control Objective One: Comprehensive procedures exist for managing insurance claims which clearly set out the roles and responsibilities of the officers involved in claims management. Staff receive appropriate training to ensure their knowledge of regulatory and other insurance-related requirements is kept up to date.	**Substantial Assurance**	-	-	1	-
Control Objective Two: All claims processed by the Council are accurately recorded on Claim Control with all relevant details noted on the system. Claim correspondence is collated with any investigation records and other documents	**Comprehensive Assurance**	-	-	-	-

relating to the claims securely stored and retained in accordance with the Council's document retention policy.					
Control Objective Three: Claims are processed promptly and efficiently in accordance with claims handling agreements and the requirements of the relevant insurer/policy with appropriate segregation of duties observed within the process particularly in relation to determining settlements and making payments.	**Substantial Assurance**	**-**	**-**	**1**	**1**
Control Objective Four: Appropriate management information and reporting arrangements are in place between the Insurance and Loss Control Team and relevant insurers. Regular reporting on the Team's claims management performance is also made to Council's senior management to allow sufficient oversight and scrutiny of claims management.	**Substantial Assurance**	**-**	**-**	**1**	**-**
TOTAL		**-**	**-**	**3**	**1**

Nature of Recommendations

The four recommendations relate to issues identified with the design of existing controls and represent instances in which the control framework requires revision to adequately address risks.

Key Findings

We identified the following areas of good practice:

- Officers involved in the claims handling process receive appropriate training to help ensure their knowledge of the industry remains current.
- The Council has claims handling agreements in place with Travelers and Zurich Municipal covering Public Liability, Motor and Property claims, resulting from competitive tendering exercises. The agreements are up to date, have been appropriately signed off and are readily available to staff.
- Completed claims are being recorded on Claim Control with all relevant details being comprehensively filled out and completed, as per our sample testing.
- The Council uses the Scottish Council on Archives Record Retention Schedule.
- Relevant records and documents relating to claims are being properly linked to the corresponding claims in the Claim Control system, as per our sample testing.

- There are established reporting procedures in place between the Council and the insurers to help ensure appropriate oversight of the claims management process.

- There are arrangements in place to ensure that claims management is regularly discussed to allow for sufficient oversight.

We have identified the following areas for improvement:

- There is not a single Claims Management Handbook in place which comprehensively covers the claims handling process or formally sets out roles and responsibilities.

- The quarterly file reviews process could be strengthened and formally documented in a Claims Management Handbook, to help ensure all claims are actively monitored and addressed.

- Further guidance should be provided around the differing authorisation limits for the different payment systems.

- Management should consider implementing a structured reporting arrangement whereby the Insurance team provides updates to senior management on claims activity and performance.

Impact on Risk Register

No specific risks relating to insurance are listed in the Council's Corporate and Service risk registers.

(v) INTERNAL AUDIT REPORT 2024/08

Client	**Corporate Services – People Service**
Subject	**Payroll – Changes in Circumstances**

Executive Summary

Conclusion

Substantial Assurance
The Council has established effective processes for managing changes to employee circumstances with appropriate controls for verification and authorisation. Our review identified several areas for improvement, though these are relatively minor in nature and many are already being addressed by management. Implementing our recommendations will complement these ongoing initiatives and further strengthen the control environment for processing payroll changes accurately and efficiently.

Background

The Payroll Team within Corporate Services - People Services is responsible for administering the salaries and expenses for approximately 7,300 monthly-paid City Council employees and 950 employees of various external organisations. The Tayside Pension Fund, serves a total membership of 56,905, including 18,765 active members, 18,645 pensioners, and 19,495 deferred/undecided/frozen members.

For the 2024/25 financial year, the Council has budgeted for 6,312 full-time equivalent staff, with staff costs in the final revenue budget set at £284,361,000. This represents a substantial increase from the previous year's budget of £263,570,000, reflecting the growing demands on the payroll system and the importance of accurate, timely processing of changes in employee circumstances.

The payroll function utilises several key processes and systems, including Firmstep for capturing changes in employee circumstances, and Resource Link as the primary HR and payroll calculation system. These systems are crucial in managing various salary sacrifice schemes, pension contributions, and processing leavers and new starters.

Scope

Review of the processes by which information affecting individual's pay calculation is notified and actioned. To include pension contributions and salary sacrifice schemes.

Objectives

		Action Priority			
		C	H	M	L
Processes and controls are in place to ensure that changes in employee circumstances are accurately captured, validated, and promptly processed in the payroll system	**Substantial Assurance**	-	-	1	1
Salary sacrifice schemes and pension contributions are managed effectively, with proper authorisation, timely implementation, and accurate payroll adjustments	**Substantial Assurance**	-	-	1	-
The leavers process includes adequate controls to prevent overpayments, with any occurrences promptly detected and appropriately managed	**Substantial Assurance**	-	-	1	1
Management information is regularly compiled and reported to identify issues, monitor the accuracy of payroll processing, and highlight developing risks related to changes in employee circumstances	**Substantial Assurance**	-	-	2	-
TOTAL		-	-	5	2

Nature of Recommendations

Four (3 medium, 1 low) of the recommendations relate to the design of controls, and three (1 low, 2 medium) to the operation of existing controls. This suggests that the control framework itself requires revision to adequately address the risks identified.

Key Findings

The Payroll Team is implementing a number of planned improvements and enhancements to processes. We have noted that these are underway where relevant in the course of assessing the effectiveness of existing controls and taken these into consideration in drafting our recommendations. These include:

- Migration of all processes relating to notification of changes in circumstances to the electronic Firmstep platform, replacing those remaining procedures which include or rely on standalone forms.
- Ongoing review of policies and guidance made available to employees through OneDundee.
- Development of a centralised repository for policy and process information, as part of the wider migration to SharePoint.

- Migration of processes relating to Pension Additional Voluntary Contributions (AVCs) to an electronic system that interfaces directly with the systems of Tayside Pension Fund.

We identified a number of areas of good practice:

- Changes to employee working arrangements are processed through a digital workflow system which enforces completion of all required steps and all required approvals before changes take effect.

- There are clear timelines and monitoring processes for Payroll changes and an established approach for prioritising urgent cases.

- Only authorised staff have access to the payroll systems and user access is periodically reviewed.

- Applications for salary sacrifice schemes undergo an eligibility assessment before they are approved, including verification of affordability criteria and confirmation that deductions would maintain salary levels above national minimum wage requirements.

- Administration of pension contributions and any changes follow structured processes with established controls and reconciliation procedures.

- Final payment calculations utilise information automatically pulled from Resource Link, with payroll staff performing calculations for different employee categories.

- A framework exists for managing salary overpayments which is supported by defined policies and procedures, aligned with the Employment Rights Act 1996.

- Established pension administration processes have been implemented for leavers, with regular communication occurring between the Payroll and Pensions teams.

- Exception reporting provides effective control through the review and investigation of payroll anomalies, with tracking of resolutions and escalation protocols for complex cases.

We have identified the following areas for improvement:

- While core payroll processes are sound, there are issues with how forms and guidance for employees are organised and accessed on One Dundee, which could lead to inefficiencies and potential errors. Removing outdated versions from the intranet and introducing a planned review cycle will reduce the risk of staff attempting to follow obsolete processes.

- There are no formally defined procedures for payroll staff processing changes in employee circumstances. Documenting key processes and establishing a central repository for this information will enhance consistency and reduce the possibility of error.

- Reconciliation processes have been implemented for salary sacrifice schemes; however, documentation could be strengthened by recording their outputs in such a way that managers approving payments to scheme providers can quickly verify that reconciliations have been carried out in advance of payment.

- The leavers process is reliant on managers notifying Payroll that a person intends to leave or retire. Analysis of 2024 data identified delays in leaver notifications across services creating a risk of payroll processing errors and potential overpayments. While this is partially mitigated by other preventative controls, introducing a means to feedback details of late notifications to Service Management could help to reduce the frequency of these errors.

- Payroll processing KPIs show high performance levels but have limitations in scope and utilisation. KPIs should be reviewed to ensure that the purpose for which they are being recorded is clear, including where they are reported and the extent to which they support management decision making.

- Recent organisational changes have created uncertainty around responsibility for risk management processes for payroll operations, impacting the effectiveness of risk assessment and prioritisation. Management should ensure that this responsibility is clearly allocated, and that Payroll risks are subject to regular review.

Impact on risk register

The People risk register included, at time of audit, the following risks:

- CSPS003 IT Systems Failure (Internal / External) (Inherent risk 5x4, residual risk 4x4)
- CSPS004 Finance (Inherent risk 4x5, residual risk 4x3)
- CSPS005 Legal / Legislative (Inherent risk 5x2, residual risk 4x2)

Our review considered these risks from the perspective of payroll change of circumstances processes, data validation controls, and compliance with payroll regulations.

The principal controls documented in the risk register include "Support & maintenance in place for all systems" for CSPS003 and "Financial monitoring and reviews in place" for CSPS004, which is rated as fully effective. Our audit confirmed that financial controls for payroll processing are generally robust, with effective exception reporting and verification processes in place.

We identified overpayment risks due to delayed notifications of changes in employees working circumstances as a potential concern, with 44 instances recorded since January 2024. While this would conceptually fall under CSPS004, the current risk description focuses on funding constraints rather than payroll accuracy, potentially leaving this specific risk area underrepresented in the risk framework.

Given that the risks mentioned above are beyond their scheduled review date, as identified in our recommendation regarding risk management framework, risk owners should reassess whether the current residual risk ratings accurately reflect the present control environment.

(vi) INTERNAL AUDIT REPORT 2023/17

Client	**Neighbourhood Services and Corporate Services – Customer Services and IT**
Subject	**Civica Cx – Rent Accounting Module**

Executive Summary

Conclusion

Substantial Assurance
The implementation of the Civica Cx Rent Accounting module has established a robust foundation for managing council housing rents across over 12,500 properties since February 2021, through effective core processes and controls. The system implementation established automated processes for rent calculations, payment handling, and arrears management, with appropriate controls ensuring accurate processing of the Council's annual rental income. The core financial processes demonstrate sound design through automated workflows and reconciliation procedures, particularly for Housing Benefit and Universal Credit management. While operational controls have been implemented effectively, the project significantly overran its original 2018 implementation date and involved significantly more input from officers and the contractor than anticipated. Changes to the timetable were managed through project management processes, and some mechanisms were put in place to carry lessons learned into subsequent phases, however we noted that no formal exercise to identify the reasons for the delay has been carried out. Although out with the scope of this audit, we note that despite carrying forward some lessons, implementation of subsequent modules has also been significantly delayed, and as a consequence the integrated system that was originally envisaged is still not in place. The Council's Senior Management have instigated a broader review of the project as a whole, to be undertaken by external consultants.

Background

Cx is an integrated housing management system developed by Civica. The software consists of a set of semi-independent modules which support specific housing management processes, such as Rent Accounting, Allocations, Asset Management, and Repairs and Maintenance. Modules can be implemented separately but also integrated with each other and with other Civica products used by the Council such as the general ledger system Civica Financials.

The Council is engaged in a project which aims to implement Civica Cx as an integrated system to support housing management business processes. The implementation of the system has been split into a number of phases, which will incrementally deploy the required modules throughout the life of the project.

The first phase of the project related to the implementation and integration of the Rent Accounting module and went live in February 2021. This is designed to support the collection

and administration of rents and applicable benefits, and their recording in the Council's financial management systems. Further phases were planned to be built and deployed throughout 2023/24.

The Council collected £55.2m in dwelling rents across over 12,500 properties throughout 2023/24. To comply with Legislation and Accounting guidance applicable to Local Authorities, these transactions must be separately accounted for through the Housing Revenue Account. It is therefore essential that the processes implemented as Phase 1 of the Civica Cx programme have embedded and are operating effectively.

Scope

Review of the arrangements for the implementation of Phase 1 of Civica Cx incorporating Housing Rent collection and recording of Housing Benefit / Universal Credit housing costs.

This review did not consider the transition arrangements for the transfer of information between the legacy system and the newly implemented system, or other phases of the Civica Cx implementation project.

Objectives

		Action Priority			
		C	H	M	L
Rents for Council tenants are accurately calculated and billed through the Civica Cx Rents module.	**Comprehensive Assurance**	-	-	-	-
Applicable housing benefits and Universal Credit are correctly received, recorded, and allocated.	**Comprehensive Assurance**	-	-	-	-
There are effective processes in place to monitor and manage rent collection.	**Comprehensive Assurance**	-	-	-	-
The planned deliverables of Phase 1 of the Civica Cx project have been implemented and embedded.	**Limited Assurance**	-	1	-	-
TOTAL		-	1	-	-

Nature of Recommendations

One high recommendation relates to the design of controls and reflects observations relating to the broader framework which supports implementation of Civica Cx project phases. We have not identified any issues with the processes implemented for Rent Accounting.

Key Findings

Implementation of the Rent Accounting Module of Civica Cx was originally planned to go live in 2018 but was not implemented until 2021. Although the scope of this review was confined to Rent Accounting and its underpinning processes, we have considered the implications for subsequent phases of the Civica Cx implementation project under Objective 4.

We have raised a recommendation to the effect that project management processes are revised to include a formal process of post implementation review in order to provide stronger assurance that the project deliverables have been achieved and that project management in place is effective.

The Council's Senior Management have instigated a broader review of the project as a whole, to be undertaken by external consultants. The scope of the external review is broader than the post implementation review that we have recommended, and as such we expect that the conclusions it reaches regarding the wider project will be applicable to this project phase.

We identified a number of areas of good practice within the processes implemented for Rent Accounting:

- The creation and maintenance of tenant accounts is governed by documented procedures and system controls, with clear staff responsibilities for verification and oversight.

- Rent charges and collections are managed through automated processes with appropriate controls and multiple payment options to support effective rent collection.

- The annual rent review process follows statutory requirements and established procedures beginning with tenant consultation in November/December, followed by committee approval in January.

- Housing Benefit and Universal Credit payments are processed through automated workflows with tracking and verification controls to ensure payments are accurate.

- Financial data transfer between housing management and financial management systems operates through controlled batch processing, with daily distribution of reconciliation reports and documented investigation procedures for resolving variances.

- Rent arrears and collection performance are monitored through a combination of system-generated reports and predictive analytics tools, enabling both systematic identification of arrears cases and targeted intervention strategies.

- The progression of arrears cases follows a framework, which includes automated weekly reviews, mandatory authorisation points and documentation requirements that ensure consistent application of policy.

- Repayment arrangements for rent arrears are managed through system-enforced steps that ensure all required information is captured and arrangements are properly tracked.

- The implementation of Civica Cx Phase 1 was subject to a formal project management approach, supported by documentation and monitoring systems.

- There is a framework established for training and supporting users of the Civica Cx System combining centralised and team-level support, utilising multiple delivery

methods and maintaining current documentation to ensure there is sustainable adoption of the system.

We have identified the following area for improvement:

- While there is evidence of ongoing testing and refinement through project planning meetings and system testing in both test and live environments, the absence of formal post-implementation review means that the root causes of the significant implementation delay have not been clearly identified. As a consequence, no assurance can be gained that systems of project management operated effectively for this project phase.

Impact on risk register

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

- DCC001 Financial Sustainability (inherent risk 5x4, residual risk 5x4)
- CSCS001 Budget/Finance (inherent risk 5x4, residual risk 5x3)
- CSCS003 IT/Systems (inherent risk 5x3, residual risk 4x2)
- CSCS009 Transformation/Change Management (inherent risk 4x3, residual risk 3x3)

The Council uses Civica Cx to manage its annual rental income of £55.2m, making the system a key control in maintaining financial sustainability.

The most significant risks identified in the risk registers relate to financial sustainability and system effectiveness. Our review considered these risks from the perspective of payment processing accuracy, system integration, and the ability to demonstrate effective rent collection and arrears management.

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

- System workflows and automated validations
- Financial reconciliation procedures
- Monitoring and reporting frameworks
- Change management processes

Our review found these controls to be operating effectively, with robust frameworks in place for payment processing, arrears management and system governance.

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.