The Highland Council

Agenda Item	**3**
Report No	**AC/19/26**

Committee: **Audit Committee**

Date: **11 November 2026**

Report Title: **Internal Audit Reviews and Progress Report – 01/08/26 – 27/10/26**

Report By: **Strategic Lead (Audit and Risk)**

1. Purpose/Executive Summary

1.1 This report provides details of the work undertaken by the Internal Audit section since the last report to Committee in August 2026.

2. Recommendations

2.1 Members are asked to:

i. **Consider** and **note** the Final Reports referred to in Section 5.1 of the report.
ii. **Scrutinise** and **note** the current work of the Internal Audit Section outlined at sections 6 and 7, and the status of work in progress detailed at **Appendix 1**.
iii. **Note** that an additional audit has been agreed and is in progress relating to Common Good Fund – Review of Events and Festivals.

3. Implications

3.1 Risk - the risks and any associated system or control weaknesses identified as a result of audit work or corporate fraud investigations will be reviewed and recommendations made for improvement.

3.2 Resources – There are currently two vacancies within the Internal Audit Team – Auditor and a Trainee Auditor both are subject to recruitment. Further information is provided in section 6.1.

3.3 There are no Legal, Health and Safety or Gaelic implications arising from this report.

4. Impacts

4.1 In Highland, all policies, strategies or service changes are subject to an integrated screening for impact for Equalities, Poverty and Human Rights, Children's Rights and Wellbeing, Climate Change, Islands and Mainland Rural Communities, and Data Protection. Where identified as required, a full impact assessment will be undertaken.

4.2 Considering impacts is a core part of the decision-making process and needs to inform the decision-making process. When taking any decision, Members must give due regard to the findings of any assessment.

4.3 This is an update report and therefore an impact assessment is not required.

5. Internal Audit Reports

5.1 There have been 4 reports issued during this period as detailed in the table below.

Service Cluster	Subject	Audit opinion
Place	Ferries	Substantial Assurance
Corporate	IT Infrastructure (Data Centre)	Substantial Assurance
Corporate	Payroll	Reasonable Assurance
Corporate	Payroll Mandate Fraud	Limited Assurance

Each report contains an audit opinion based upon the work performed in respect of the subject under review. The five audit opinions are set out as follows:

(i) Full Assurance: There is a sound system of control designed to achieve the system objectives and the controls are being consistently applied.
(ii) Substantial Assurance: While there is a generally a sound system, there are minor areas of weakness which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.
(iii) Reasonable Assurance: Whilst the system is broadly reliable, areas of weakness have been identified which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.
(iv) Limited Assurance: Weaknesses in the system of controls are such as to put the system objectives at risk, and/ or the level of non-compliance puts the system objectives at risk.
(v) No Assurance: Control is generally weak, leaving the system open to significant error or abuse, and/ or significant non-compliance with basic controls leaves the system open to error or abuse.

6. Internal Audit work in progress and staff resources

6.1 During October, the Internal Audit Team experienced two staffing changes, resulting in an Auditor moving to a post within Corporate Finance and the departure of the Trainee Auditor. Recruitment to these vacant posts is actively progressing. Interviews for the Auditor post are scheduled for late October 2026, while the Trainee Auditor post is currently being advertised, with a closing date for applications of 2 November 2026.

In the interim, the resources available to deliver the approved Internal Audit Plan have been significantly reduced. To maintain service delivery and conclude audit work already in progress, assignments have been reallocated across the existing team. While recruitment is progressing, appointment and start dates for successful candidates cannot yet be confirmed and, consequently, there may be a period before staffing levels return to full capacity.

The impact on audit coverage and delivery timescales is being closely monitored, with mitigating actions being taken where possible.

6.2 Audits for the 2026/27 audit plan are in progress, and their current status is provided at **Appendix 1**. The Internal Audit Team has continued to make best efforts to ensure timely completion of this audit work.

6.3 Since the last Audit Committee an additional unplanned audit has been agreed by the Strategic Lead. This relates to Inverness Common Good Fund – Review of Events and Festivals and this has been added to the list of audits at Appendix 1.

7. Other Work

7.1 The Section has been involved in a variety of other work during the period which is summarised below:

- Audits for other Boards, Committees and Organisations

  Audit work has been undertaken during this period for the Valuation Joint Board, Pensions Board and for High Life Highland which will be reported to the respective Boards/ Committees in due course.

- Attendance at HR & Payroll Programme Board

  Audit representation has been requested on the Board in an independent non-voting capacity. The role being carried out by the Corporate Audit Manager is to act as the "critical friend" to assist in providing assurance in matters relating to internal controls, governance and risk management.

- Attendance at officer meetings for Inverness Green Freeport

  Developing preparatory understanding of arrangements surrounding the role of the Highland Council as Accountable Body for the Inverness Green Freeport. The Green Freeports Framework sets a range of new expectations and assurance requirements including additional internal audit reporting requirements.

  In addition to the above, the first annual internal audit of the Inverness Green Freeport has commenced.

- Global Internal Audit Standards (GIAS) update

  Members will be aware that the Internal Audit Annual Report 2025/26 included an internal assessment of conformance against the GIAS. This identified two areas of non-conformance which were detailed within an action plan. These actions have been progressed as follows:

  (1) The work to review and update the Audit Manual has been completed (target date was 31/07/27).
  (2) The External Quality Assessment has been scheduled and will be undertaken by Glasgow City Council. This review will commence in November, and the report will be presented to the next Audit Committee meeting in March 2027. This will ensure that the action target date of 31/03/27 is achieved.

- Staff training and development

  To support continuous professional development and maintain compliance with the Global Internal Audit Standards (GIAS), members of the Internal Audit team attended the online Chartered Institute of Internal Auditors Annual Conference. Attendance provided exposure to emerging internal audit practices, growing role of AI in internal audit, regulatory developments, as well as governance and risk management insights from peers across the public and private sectors.

- Attendance at the Scottish Local Authorities Chief Internal Auditors Group (SLACAIG) meetings

  The Council is a member of SLACAIG with the Strategic Lead (Audit & Risk) attending the quarterly meetings. In addition, there are also two sub-groups for Digital Assurance and Investigations which are attended by members of the Corporate Audit Team.

  The Strategic Lead (Audit & Risk) is also a member of the Management Committee and a member of the External Quality Assessment Moderation Panel.

- Corporate Fraud, Whistleblowing concerns and other investigations activity

  The Single Point of Contact (SPOC) work is an ongoing commitment providing information to Police Scotland, the Department of Work and Pensions and the UK Immigration Enforcement Office. This work assists these organisations in investigating potential crimes and in making our communities safer. An allowance of time for these commitments is made within the Internal Audit Plan each year. We have seen an increase in activity in this area over the last reporting period.

  At the end of September 2026, we have a current commitment of 12 cases. This comprises of several active cases subject to investigation and those where the investigation has been concluded but there is ongoing recovery or has been reported to the Procurator Fiscal. A summary of the cases are as follows:

  - Eight ongoing Whistleblowing cases.
  - One Payroll Mandate Fraud (A weakness report was prepared and the final report has now been issued as referenced at section 5.1 above).
  - Three ongoing investigations, two reported by the Service, one externally reported.

  Where active fraud and whistleblowing investigations are in progress, no further information can be provided in order to prevent these being compromised. However, once the investigations have been completed including any associated disciplinary/ legal action where relevant, the control weaknesses reports will be provided to the Audit Committee to scrutinise.

8. CIPFA Audit Committee Guidance 2026

8.1 CIPFA published updated guidance Audit Committees: Practical Guidance for Local Authorities and Police in October 2026. This replaces the 2022 edition which has informed the current Audit Committee arrangements.

8.2 The updated guidance will necessitate a review of the current Audit Committee arrangements to ensure that we comply with best practice as set out by CIPFA. However, as there is only one remaining Audit Committee meeting for the current Council, this work will be undertaken for the new Council, post May 2027.

Designation: Strategic Lead (Audit and Risk)

Date: 27 October 2026

Authors: Donna Sutherland, Strategic Lead (Audit and Risk)
Jason Thurlbeck, Corporate Audit Manager

Appendices: Appendix 1 – 2026/27 Internal Audits in progress

Appendix 1

Internal Audit Plan 2026/27

Audits in progress:

Service Cluster	Audit Area	Priority	Audit Days	Current Status	Planned Committee Reporting Date
Corporate	Legal Services	Medium	30	Draft Report	March 2027
People	Additional Support for Learning	Medium	30	Substantially complete	March 2027
Place	Roads Operations and Maintenance	High	30	Substantially complete	March 2027
Place	Property Capital Projects	High	30	Fieldwork in progress	March 2027
Corporate	Review of Exit Packages	n/a	n/a	Fieldwork in progress	March 2027
Place	Economy & Regeneration	Medium	30	Planning completed	March 2027
Place	Inverness and Cromarty Firth Green Freeport	High	30	Fieldwork Underway	March 2027
People	Family Teams - Whole Family Wellbeing Fund	Medium	30	Planning completed	March 2027
Place	Inverness Common Good Fund – Review of Events and Festivals	n/a	10	Planning completed	March 2027

Audits to be allocated:

Service Cluster	Audit Area	Priority	Audit Days	Current Status	Planned Committee Reporting Date
Corporate	Strategic Improvement	Medium	30		
Corporate	Insurance	Medium	30		
Corporate	Data Protection	High	30		
Corporate	Human Resources – Work Force Planning	Medium	30		
Place	Building Maintenance	Medium	30		
Place	Housing Development	Medium	30		
Corporate	Risk Management	Medium	30		
People	Family Teams - Self Directed Support	Medium	30		
People	Secondary Schools - Employability Services	Medium	30		

Service Cluster	Audit Area	Priority	Audit Days	Current Status	Planned Committee Reporting Date
Place	Environmental Health	Medium	30		
People	Fostering and Adoption - Families First	Medium	30		
Corporate	Debtors	Medium	30		
Place	Harbours	Medium	30		
Reserves					
People	Family Teams - Child Plans	Medium	30		
Place	Street Lighting and Communications	Medium	30		
Corporate	Governance of Arms-Length External Organisations	Medium	30		

* Once the Terms of Reference has been prepared, this will detail the planned Committee reporting date.

Internal Audit Final Report

Place Cluster

Ferries

Description	Priority	No.
Major issues that managers need to address as a matter of urgency.	High	0
Important issues that managers should address and will benefit the Organisation if implemented.	Medium	1
Minor issues that are not critical but managers should address.	Low	2

Audit Opinion

The opinion is based upon, and limited to, the work performed in respect of the subject under review. Internal Audit cannot provide total assurance that control weaknesses or irregularities do not exist. It is the opinion that **Substantial Assurance** can be given in that while there is generally a sound system, there are minor areas of weakness which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

Distribution:
Assistant Chief Executive, Place
Chief Officer, Facilities & Fleet Management
Principal Transport Officer
Operations Manager, Corran Ferry
Audit Scotland

Draft Date: 16/10/26
Final Date: 28/10/26

1. Introduction

1.1 The Highland Council operates and oversees ferry services which provide important transport links for communities, businesses and visitors throughout the Highlands. This includes the Council operated Corran Ferry service together with five ferry routes delivered by external contractors on behalf of the Council.

1.2 The Corran Ferry provides a vital transport link across Loch Linnhe and is heavily relied upon by local residents, commuters and visitors. The service continues to operate within a challenging financial and operational environment, with increasing operating costs, ageing infrastructure and limited contingency arrangements. As a result, effective management of income generation and service delivery remains critical to the sustainability of the service. Budgeted income from the Corran Ferry for 2026/27 was £2.216 million.

1.3 The Corran Ferry is a strategic transport priority for Highland Council with a significant project underway to deliver a new electric ferry and infrastructure upgrades by early 2029. The new electric ferry aims to deliver a modern, reliable and sustainable service on Scotland's busiest single-vessel ferry route.

1.4 A key component of the Corran Ferry operation is the ticketing system, which supports both revenue collection and access to the service. The current ticketing arrangement involves fares being collected by Pursers on board the vessel using the Compass ticketing system, with customers also able to purchase discounted ticket books either on board or at selected Council offices. The accuracy, reliability and control framework surrounding ticketing and income collection are therefore important in ensuring that all revenue due to the Council is appropriately collected, recorded and banked.

1.5 A revised ticketing project was underway to enhance the existing Corran Ferry ticketing system by introducing online ticket sales. Passengers will be able to purchase digital tickets online and present a QR-code on their smartphone for validation by the ferry Purser. The system is expected to be operational by December 2026 to January 2027.

1.6 The audit examined the design and operation of the current Corran Ferry ticketing system, including ticketing processes, staffing arrangements, customer accessibility, income collection, reconciliation and management reporting. The review also considered whether ticketing information and passenger data were used effectively to support operational and financial decision making.

1.7 In addition, the audit considered the Council's oversight arrangements for contracted ferry services delivered by third party operators. Testing focused on procurement and contract management arrangements, review of service requirements prior to procurement, performance monitoring, contractor reporting, and the processes in place to ensure service issues and performance concerns were appropriately managed. The review sought to determine whether sufficient oversight arrangements were in place to support service delivery, maintain appropriate standards and provide value for money for the Council and service users.

2. Main Findings

2.1 *The Corran ferry ticketing system is appropriately designed and implemented to meet operational requirements and satisfactory customer experience.*

This objective was substantially achieved. Testing confirmed that approved fares were applied through the Compass ticketing system and that arrangements were in place to issue tickets, collect fares and record passenger and vehicle information. Ticketing was observed in operation during the site visit and was found to be practical and accessible for users, with no significant delays or operational issues identified during the observation period. Staff demonstrated a clear understanding of their responsibilities and appropriate arrangements were in place to support service delivery and customer experience.

Staffing arrangements supporting the operation of the ticketing system were also found to be effective. Staffing levels were guided by Maritime and Coastguard Agency (MCA) minimum manning requirements and operational considerations, with additional seasonal staffing utilised during periods of increased demand. Overtime arrangements were supported by documented justification and approval processes, providing assurance that additional staffing resources were used appropriately and subject to management oversight.

Management received and reviewed information relating to passenger volumes, fare income and service usage through the Compass ticketing system and supporting management reporting arrangements. Information was monitored through budget monitoring processes, management review meetings, stakeholder engagement activities and performance reporting arrangements, enabling service usage, revenue performance and operational trends to be monitored effectively.

However, whilst ticketing responsibilities, operational guidance and supporting controls were documented across a number of sources, there was currently no single documented procedure describing the complete end to end ticketing process. This increased reliance on staff knowledge and reduced process resilience in the event of staff turnover or operational change (See Action Plan Ref L1).

Overall, the Corran Ferry ticketing arrangements were found to be operating effectively and supporting the operational requirements of the service. Appropriate controls were in place to support accurate ticketing and passenger recording, and management information was available to support service oversight. The recommendation identified represents an opportunity to strengthen documentation, improve process resilience and support the consistent application of controls.

2.2 *Revenue generated through ticketing for the Corran ferry is accurately recorded, securely handled, and subject to robust financial controls, ensuring transparency, accountability, and compliance with relevant policies and procedures.*

This objective was partially achieved. Revenue generated through the Corran Ferry ticketing system was subject to established financial controls and was generally recorded, reconciled and banked appropriately. Testing confirmed that income was supported by documented reconciliation processes, banking controls and audit trails. Appropriate oversight arrangements were in place, with management receiving regular information relating to passenger volumes, ticket sales and fare income. Training, familiarisation and supervision arrangements were also evidenced for staff involved in ticketing, income collection and income recording activities.

Ticketing equipment was supported through documented maintenance arrangements, supplier support contracts and fault reporting processes. Contractual support arrangements were in place with the system supplier and testing confirmed that equipment issues were logged, tracked and resolved through formal support mechanisms.

Review of reconciliation processes found that, for the majority of the 20 pay-in records tested, ticketing reports, daily reconciliation records and bank deposit information were consistent and supported by appropriate documentation. However, testing identified four small discrepancies totalling £189 (0.19% of the total sample value of £101,437.50) within the sample reviewed. Whilst explanations had been recorded for some variances, supporting evidence was not consistently retained and in several instances, comments stated that differences "may" relate to a particular cause rather than providing a confirmed explanation. As a result, the audit trail supporting reconciliation activities was weakened and management assurance over the investigation and resolution of variances was reduced (See Action Plan Ref L2).

In addition, the review identified an opportunity to strengthen physical security arrangements relating to cash and ticket stock. Whilst secure storage facilities are available and controls were generally in place, the review found opportunities to improve the restriction of access and the consistent application of security controls. Consideration should therefore be given to reviewing

access permissions and ensuring that security arrangements are practical and consistently applied (See Action Plan Ref M1).

Overall, income collection and financial control arrangements were found to be operating effectively, and no material issues were identified regarding the recording, reconciliation or banking of ferry income. However, opportunities exist to strengthen both the documentation of reconciliation differences and the physical safeguarding arrangements for cash and ticket stock. Addressing these areas would further improve accountability, strengthen the audit trail and reduce risk of errors or unauthorised access.

2.3 *The Council maintains appropriate oversight of ferry service, including those delivered under contract, to ensure appropriate service standards are met.*

This objective was fully achieved. The review found that the Council maintains appropriate oversight of ferry services delivered by external providers. Evidence was available to demonstrate that service requirements were considered and documented prior to procurement activity being undertaken. Procurement business cases, consultation records and approval documentation demonstrated that operational requirements, stakeholder needs, procurement options, risks and financial implications were reviewed before requirement and contract extension decisions were made.

Appropriate procurement governance arrangements were also found to be in place. Procurement activities were supported by formal approval processes and the involvement of the Commercial & Procurement Shared Service. Documentation reviewed demonstrated that procurement activity was subject to established governance arrangements and appropriate approval before contracts were awarded or extended.

The review also found that contract specifications were reviewed prior to retendering and took account of operational requirements, service demand and stakeholder feedback. Consultation evidence, contract variation records and procurement documentation demonstrated that service requirements were actively considered and reviewed rather than simply renewed without challenge.

Contractors provided operational and performance information to the Council, including passenger statistics, vehicle carryings, revenue information and operational performance data. This information was used to monitor service delivery, identify operational issues and support contract management activities. Evidence was also available to demonstrate that the Council maintains arrangements to identify and respond to service concerns through contractor reporting, stakeholder engagement and community consultation activities.

Overall, appropriate procurement, governance, contract management and performance monitoring arrangements were found to be operating across contracted ferry services. The Council was able to demonstrate effective oversight of contracted operators to deliver value for money for the Council and service users, supported by documented procurement processes, contractor reporting arrangements and service review activities.

3. Conclusion

3.1 The audit provided substantial assurance that appropriate processes and controls were in place across all three objectives reviewed and were generally operating as intended. Good practice was evident in the operation of the Corran Ferry ticketing system, the management of fare income and the governance arrangements supporting contracted ferry services. Testing confirmed that ticketing, income collection, reconciliation and banking arrangements were supported by established procedures and management oversight, while procurement, contract management and performance monitoring arrangements were found to provide appropriate oversight of externally operated ferry services.

However, opportunities for improvement were identified in relation to the documentation of ticketing processes, the consistency of reconciliation evidence and the physical security arrangements surrounding cash and ticket stock. These issues do not undermine the overall control environment, and no significant weaknesses were identified in relation to the collection of income, operation of ticketing controls or oversight of contracted ferry

services. Nevertheless, if left unaddressed, they may reduce process resilience, weaken the supporting audit trail and increase exposure to avoidable control risks over time.

Overall, the audit concluded that the Council had appropriate arrangements in place to operate and oversee ferry services, and that the controls reviewed were generally effective in supporting service delivery, accountability and value for money. The recommendations identified within this report are intended to further strengthen existing arrangements and support the continued effective management of ferry services.

4. Action Plan

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	**Target Date**
M1	Medium	Access to cash and ticket book stock was shared across several staff, including cover arrangements, and in some circumstances physical security was reduced where staff were unfamiliar with its operation. While this reflected practical operational considerations, it reduced the effectiveness of control over access to cash and ticket stock.	Physical security arrangements for cash and ticket stock at Corran ferry should be reviewed to ensure that access is appropriately restricted and controls are consistently applied.	Immediately, physical security arrangements for cash and ticket stock at Corran ferry shall be reviewed to ensure that access is appropriately restricted and controls are consistently applied.	Operations Manager, Corran Ferry	13/11/26
L1	Low	Whilst ticketing guidance and staff responsibilities were documented, the information was contained across a number of documents and did not provide a single, comprehensive procedure describing the end-to-end ticketing process or the controls used to ensure all chargeable ferry users were appropriately identified, charged and reconciled.	The service should develop and maintain a documented end to end ticketing procedure which clearly describes ticket issuance, fare collection, passenger and vehicle recording, waybill completion, reconciliation activities and the controls used to ensure all chargeable ferry users are appropriately accounted for.	Within 6-months, the service will develop and maintain a documented end to end ticketing procedure which clearly describes ticket issuance, fare collection, passenger and vehicle recording, waybill completion, reconciliation activities and the controls used to ensure all chargeable ferry users are appropriately accounted for. Coinciding with the new online ticketing, this timing allows the new online ticketing systems to be fully launched and documented.	Operations Manager, Corran Ferry	30/04/27
L2	Low	Four small discrepancies were identified in testing of income records. Whilst explanations had been recorded for some variances, supporting evidence was not consistently retained	Management should ensure that all reconciliation differences are fully investigated and documented. Explanations should clearly state the confirmed cause of any variance	Immediately, management will ensure that all reconciliation differences are fully investigated and documented. Explanations will clearly state the confirmed cause of any variance and be	Operations Manager, Corran Ferry	13/11/26

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	Target Date
		and in certain instances comments recorded against differences stated that the variance "may" have related to a particular item rather than confirming the actual cause of the discrepancy.	and be supported, where appropriate, by sufficient evidence to demonstrate how the discrepancy was resolved. Use of speculative explanations such as "may be due to" should be avoided where possible, with outstanding variances formally investigated until a definitive explanation is obtained or the matter is appropriately escalated.	supported, where appropriate, by sufficient evidence to demonstrate how the discrepancy was resolved. Use of speculative explanations such as "may be due to" will be avoided where possible, with outstanding variances formally investigated until a definitive explanation is obtained or the matter is appropriately escalated.		

Internal Audit Final Report

Corporate Cluster

ICT Infrastructure- new data centre footprint

Description	Priority	No.
Major issues that managers need to address as a matter of urgency.	High	0
Important issues that managers should address and will benefit the Organisation if implemented.	Medium	1
Minor issues that are not critical but managers should address.	Low	0

Audit Opinion

The opinion is based upon, and limited to, the work performed in respect of the subject under review. Internal Audit cannot provide total assurance that control weaknesses or irregularities do not exist. It is the opinion that **Substantial Assurance** can be given in that while there is generally a sound system, there are minor areas of weakness which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

Distribution:
Assistant Chief Executive, Corporate
Chief Officer, Business Solutions
Strategic Lead, ICT
ICT Operations Managers
ICT Manager, Data Centre
Programme Manager, Strategic Improvement

Draft Date: 01/10/26
Final Date: 09/10/26

1. Introduction

1.1 The Highland Council's Information and Communication Technology (ICT) Strategy 2022-2027 sets a high level vision to *'Ensure that the right technology, with the right support, is in place to enable effective service delivery, enriched learning, collaboration and informed decision making for our workforce, partners, citizens, businesses and visitors'.* To deliver these aims a portfolio of ICT projects had been initiated. This was being delivered in 5 tranches, each of which covered several individual projects.

The Tranche 4 Data Centre Migration project reviewed involved the transition from Council-owned and managed data centre infrastructure to an externally provided data centre and cloud-hosting service. The main rationale for this particular project was to address the Council's corporate risk (HRC4 concerning cyber-attacks). Improving data centre resilience via this (and other projects in the portfolio) was a key mitigation.

The project required a one-off implementation cost of £330,078 together with planned annual costs of £618,461. The total contract value to the external provider was £1.612m. The contract commenced in October 2025 for 39 months

1.2 This audit reviewed the governance, risk management and controls for the project (including the post project new business as usual arrangements). This audit does not provide assurance over the technical aspects or security of the solutions implemented as part of the data centre migration project.

2. Main Findings

2.1 *There are adequate governance arrangements in place to ensure the project can deliver its aims within the specified timescale and budget.*

This objective was substantially achieved. The project's business case rationale and aims were clearly aligned to the ICT strategy. Key project documents (project brief, Project Initiation Document, business case and options appraisal) were produced which clearly set out the aims and rationale. There were clear roles and responsibilities for the project's delivery and supporting operational plans were in place (for example a milestone checker to track progress). The project was procured appropriately in accordance with the Council's Contract Standing Orders and procurement guidance.

There was an ICT Strategy Board making decisions, this met regularly and received both an overview and detailed information on the need for the project, its progress and key information from the external provider. The governance arrangements evolved and improved during the project's lifetime as a result of ICT reviewing them. The later arrangements ensured a more comprehensive definition of roles and responsibilities, clearer separation of roles at different project levels of project governance and greater evidence of minute taking and action points. These improved arrangements delivered wider benefit as they were set up to execute, manage and scrutinise all projects in the portfolio delivering the ICT strategy.

2.2 *There are adequate risk management and business continuity arrangements in place between the Council and the commissioned external provider of the new data centre.*

This objective was substantially achieved. The project had a risk register that was in accordance with the Council's risk management policy and guidance. There was evidence risks were being identified and reviewed regularly, with risks also being appropriately closed with clear justification. Risk data had been made available to the ICT Strategy Board.

However, there was now an opportunity to review the existing ICT service risk register in light of the project's closure, reflecting that for some risk areas mitigation had changed and to record new risks where greater reliance on a third party needed to be documented. From the outset of the project the ICT Service was clear about what risks needed addressing and set these out, although a more non-technical explanation of the implications, and justification for some scores on some individual risks would have allowed a better understanding of the risk impact for stakeholders without an ICT background (See Recommendation M1).

2.3 *A process is established that ensures both internal controls and vendor-based (i.e. the external supplier) controls are in place to protect the confidentiality, integrity, and availability of the Council's systems and data*.

This objective was fully achieved. The project specification clearly set out how the external provider would demonstrate that data migration and ongoing storage would protect the confidentiality, integrity and availability of data. There was a planned process for migrating all virtual servers and the data held on them, which included conducting tests prior to the migration. There was evidence the process was followed and authorised. This provided assurance that systems were operating as intended. There was also evidence that firewall configuration testing had taken place and results approved by ICT project management as was the move to the new Scottish Wide Area Network. Evidence was provided for the decommissioning of the old hardware and removal of data held on that.

2.4 *Adequate testing of project deliverables and key security controls has taken place to provide assurance that they are effective, and also that key security considerations/assurances are built into formal agreements with the external provider.*

This objective was fully achieved. There were 5 overarching project deliverables 4 of which were reviewed as part of section 2.3 above. The remaining objective involved the set-up of new business as usual arrangements. Key security requirements had been incorporated into contractual arrangements with the external provider including provisions covering information security, data protection, business continuity, access management and incident response. This was supported by external certifications and ongoing service management processes.

The controls outlined above provide reasonable assurance that security requirements were incorporated into the provider relationship and that the project was delivered as intended. Ongoing management monitoring, contract oversight, and periodic review of service performance and security compliance will be necessary to ensure that the control environment remains effective and continues to meet the Council's requirements.

3. Conclusion

3.1 The ICT team were able to demonstrate that the Data Centre Migration project had met its objectives and that appropriate arrangements were in place for the new data centre provision. There was a strong audit trail of testing and sign offs at key stages.

Evidence was found of appropriate governance, procurement, project management and risk management arrangements, together with a clear audit trail of testing, approvals and implementation activities. Key security requirements were embedded within contractual arrangements with the external provider and supported by ongoing service management processes.

The transition to externally hosted infrastructure alters the nature of some risks and increases reliance on supplier management and oversight. As such, effective contract management and ongoing review of ICT risks will be important to ensure the anticipated benefits of the project continue to be realised.

4. Action Plan

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	**Target Date**
M1	Medium	Following project closure for some risk areas mitigations recorded had changed and there were now new risks still to be recorded reflecting the move to the new data centre and cloud hosting provision. Overly technical or brief descriptions of the implications, and justification for some scores on some individual risks could reduce understanding of the risk impact for stakeholders.	The ICT Service risk register should be updated so that: • risks identified as part of the project which are still relevant are documented • new risks identified due to greater reliance on third parties are documented. Risk scores and mitigations should be explained more clearly (where possible in non-technical language) to communicate implications to stakeholders.	A new Service Risk register template will be created to provide clear risk scoring providing risk and mitigation information in a clear and concise manner: • Project risks will be reviewed and carried over if relevant to ongoing service. • A workshop will be held to review current risks and identify any new risks for them to be populated into Service Risk register. • Service Risk Register will be reviewed and updated as part of Monthly Service Review.	ICT Operations Manager	15/12/26

Internal Audit Final Report

Corporate Cluster

Payroll

Description	Priority	No.
Major issues that managers need to address as a matter of urgency.	High	2
Important issues that managers should address and will benefit the Organisation if implemented.	Medium	3
Minor issues that are not critical but managers should address.	Low	2

Distribution:
Assistant Chief Executive – Corporate
Chief Officer – HR & Communications
Strategic Lead – HR
Pay & HR Transactions Manager
Senior Applications Analyst
Strategic Lead (Resources), Integrated People Services
Workforce Planning and Staffing Manager
CO Revenues & Commercialisation
Strategic Lead (Corporate Support)

Audit Opinion

The opinion is based upon, and limited to, the work performed in respect of the subject under review. Internal Audit cannot provide total assurance that control weaknesses or irregularities do not exist. It is the opinion that **Reasonable Assurance** can be given in that whilst the system is broadly reliable, areas of weakness have been identified which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.

Draft Date: 06/08/26
Final Date: 16/10/26

1. Introduction

1.1 Highland Council employs over 10,000 people, and in the 2025/26 financial year, staff costs represented £471.7 million of the total revenue budget of £837.4 million. The Payroll Section is responsible for delivering payroll services for all Highland Council employees, as well as those employed by High Life Highland, HITRANS and the Office of the Assessor and Electoral Registration Officer.

1.2 The audit assessed the accuracy, timeliness and authorisation of payroll transactions, including statutory deductions, reconciliations between payroll, BACS and the general ledger (GL), manual inputs, emergency payments and establishment checks. It also considered compliance with relevant legislation and policies, including PAYE regulations, GDPR and Scottish Joint Council (SJC) agreements.

The audit also examined the effectiveness of internal controls and segregation of duties, focusing on system access, approval arrangements for sensitive changes, and the monitoring of exception reports and audit logs. It also considered access controls and business continuity arrangements within the ResourceLink (RL) payroll system. Previous work on payroll overpayments was considered to avoid duplication of audit coverage. A Payroll mandate fraud was reported to the Corporate Fraud Team on the 26/09/25 and so the control environment surrounding this fraud has been considered when carrying out this review.

2. Main Findings

2.1 *Payroll transactions are accurate, complete, processed promptly, and fully comply with all relevant legislation and internal policies.*

This audit objective was substantially achieved. Overall, appropriate controls were in place to ensure the accuracy of statutory payroll updates in RL, including changes to income tax, National Insurance (NI) and Statutory Sick Pay, with both ICT and Payroll undertaking documented checks and independent verification. However, there were minor weaknesses in the consistency of how Payroll recorded the checks undertaken to confirm that pay award updates had been correctly applied in RL across all pay and grading structures (see action plan L1).

Under HMRC's Real Time Information (RTI) requirements, Highland Council was required to submit payroll information to HMRC each time employees were paid. This submission contained detailed employee-level data, including pay, tax and NI contributions, together with starter and leaver information. RTI returns for 2 sampled payroll runs were examined and found to have been submitted in accordance with HMRC requirements and prior to the relevant pay dates. Evidence confirmed that the returns had been successfully accepted by HMRC and any exceptions identified during processing were appropriately investigated and resolved before submission.

A sample of 5 employee grade/spinal point changes was examined and, for all cases tested, pay rates were accurately aligned with the applicable SJC and Teacher Pay Scales. In addition, effective dates were correctly applied, ensuring that salary amendments were implemented in a timely and appropriate manner. Where applicable, back pay calculations were found to be accurate and consistent with the revised pay rates and effective dates. All sampled changes were submitted and authorised by the employee's line manager through MyView and, although not independently verified by Payroll, managers were notified once changes had been processed, providing a compensating control.

The key data protection and record management arrangements for Payroll were in place, including structured retention practices aligned to the Corporate Retention Schedule, secure approaches to bulk data transfers, and appropriate consideration of Data Protection Impact Assessment requirements for significant system changes. The organisation of records by tax year and end-of-year housekeeping processes provided a clear framework for managing retention, while existing privacy notice arrangements were considered to be covered through overarching employment contractual provisions. However, testing of retention practices and record management within RL was not undertaken and controls relied largely on manual processes.

For 2 sampled payroll runs, BACS file totals were reconciled to payroll system outputs, with appropriate segregation of duties evidenced and dual authorisation in place. Payroll journals were successfully transferred to the GL via a secure automated interface, with system-generated confirmations and independent post-processing reconciliations demonstrating the completeness and accuracy of postings.

Payments processed outside the normal payroll cycle included emergency payments to address cases of financial hardship and bounced payments requiring reissue following verification of bank details. Testing of 5 emergency payments and 5 bounced payments confirmed that all payments were appropriately authorised, accurately recorded in CiA, and paid to verified bank accounts. Emergency payments were recovered through the next payroll run and bounced payments were reissued at the correct value.

Biannual establishment checks were undertaken to validate that employees paid through payroll were aligned with the approved staffing establishment. The September 2025 exercise achieved full compliance, while the April 2026 exercise had achieved a completion rate of 86.46% as at 23/06/26, with further follow-up planned. The introduction of a checkbox within HR forms improved the visibility of actions arising from the exercise, resulting in the identification of 498 establishment changes.

2.2 *Adequate internal controls and segregation of duties exist within payroll processes.*

This audit objective was partially achieved. There were 5 active Payroll user profiles within RL, operating under a hierarchical access structure. Each Payroll user had been assigned a single role, with no instances of multiple role allocations identified.

A review of the user profiles identified that the PAYOFF profile provided extensive access across payroll processing activities, reflecting the operational requirements of a relatively small payroll team. However, this was supported by compensating controls, which were considered elsewhere in the audit. The PAYOFF profile was assigned to a number of roles within the Payroll section including Payroll Technicians, Payroll Officers and Operations Managers, to ensure payroll processing activities could be completed within strict deadlines. In addition, more junior staff, such as Modern Apprentices and Youth Trainees, were granted the profile to fulfil their training programme but were generally supervised by more experienced staff. The SUPERVISOR profile provided unrestricted access to all payroll processing functions. This level of access was assigned to the Payroll & HR Transactions Manager, together with a number of internal ICT support staff and staff from the external payroll system provider. There were some mitigating controls in place for external users, including formal contractual and confidentiality arrangements (not examined as part of the audit), periodic access reviews (most recently undertaken in March 2026), and the automatic disabling of inactive accounts after 60 days. However, no formal monitoring was in place to provide assurance that privileged access was used only for authorised purposes (see action plan M1).

A sample of 20 manual changes to employee bank details was examined. Testing confirmed that, where supporting documentation was available, bank details had been updated accurately and that requests originated from trusted or otherwise verifiable sources. However, supporting evidence could not be provided for 4 of the changes reviewed and, although management advised that all changes were subject to independent checking, no evidence of this being performed was available for any of the sampled transactions. One instance involved the transfer of bank details from an employee's existing payroll record to a new payroll record, and this type of change was not currently subject to an independent check. In addition, one discrepancy between an employee’s address information held on RL and that provided on a bank mandate was not identified or followed up. Although employees were expected to update their bank details directly through MyView, 3 of the 20 sampled changes were processed manually due to employees being unable to access the self-service system (see action plan H1).

A sample of 20 timesheets and overtime claim forms processed by Payroll was undertaken. Only 7 of the 20 forms had been

signed by an authorised manager, with a further 10 relying on email-based approval or the manager being copied into the submission email, 2 having no evidence of approval and 1 being authorised by a colleague rather than the line manager. For Education claim forms, the practice of accepting forms where the Head Teacher was copied into the submission email as evidence of approval was formally adopted during the Covid-19 pandemic and remained in operation. Inconsistency was also identified in the administration of the process, with 12 different versions of the timesheet template in use and only 11 forms converted to PDF prior to submission as required. Forms were submitted from a variety of sources, including managers, employees and administrative staff. They had been processed accurately in 18 of the 20 cases reviewed, however, 1 overpayment (£797.20) and 1 underpayment (£116.51) were identified and referred to Payroll for corrective action. In addition, manual payroll inputs were not routinely subject to independent verification, increasing the risk of processing errors going undetected (see action plan H2). The process for the completion, authorisation, submission and processing of timesheets and overtime claims involved multiple manual stages and relied heavily on manager scrutiny as the primary assurance over accuracy. Secondary detective control relied on budget holder monitoring of payroll transactions to identify any areas of concern. The manual nature of the process increased the risk of errors, as evidenced above (see action plan M2).

Exception reports were generated for each payroll run to identify unusual or potentially incorrect transactions. Review of exception reports for 2 sampled payroll runs confirmed that exceptions had been reviewed and actioned by Payroll. However, in 1 instance the review and check were completed by the same officer, and in another the evidence of supervisory review was unclear. Weekly RL audit logs were generated but were not reviewed. Although an enhanced audit reporting tool had been procured, testing identified discrepancies in the data produced and it had not yet been implemented (see action plan M3).

2.3 *Payroll systems and data are protected against unauthorised access and have backup and disaster recovery arrangements in place.*

This audit objective was substantially achieved. A review of RL payroll user access identified 58 active internal staff accounts, all of which were verified as belonging to current employees. Controls were in place to remove access through the formal leavers process and to automatically disable accounts following 60 days of inactivity, providing assurance that obsolete and dormant accounts were appropriately managed.

The Corporate Cluster Business Continuity Plan (June 2025) covered key payroll processes, including backup and recovery arrangements and contingency support through the external payroll system provider and scenario testing was undertaken in February and June 2026. However, comments within the document indicated it remained under review, and there was no clear evidence of formal approval (see action plan L2).

3. Conclusion

3.1 The audit found that key payroll controls were largely operating effectively, supporting the accurate and timely processing of payroll and compliance with statutory requirements. Appropriate arrangements were in place for payroll reconciliations, system access management, statutory updates, and business continuity, providing assurance that core payroll activities were being delivered reliably.

Opportunities for improvement were identified in areas where processes relied on manual intervention, including changes to employee bank details, timesheet and overtime processing, monitoring of privileged user access, and the review of payroll system activity. Strengthening these controls would help reduce the risk of fraud and error, improve oversight, and enhance the overall payroll control environment.

4. Action Plan

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	Target Date
H1	High	Testing of 20 manual bank detail changes identified weaknesses in record retention, independent verification and monitoring controls. Supporting evidence was unavailable for 4 transactions, no evidence of independent review was retained, and some changes were not subject to independent checking. Non-compliance with established procedures designed to ensure the accuracy and integrity of changes to bank account details increases the risk of fraudulent or unauthorised amendments resulting in financial loss and reputational damage.	(i) MyView should be established as the mandatory method for employees to add or amend their bank account details. Recurring issues that prevent employees from accessing or using MyView should be identified, investigated, and resolved to prevent the need for manual bank mandate processing, reducing risk, improving efficiency and integrity. (ii) All manual bank detail changes, including transfers of bank details from existing payroll records, should be independently reviewed and evidenced. (iii) A programme of monitoring should be implemented prior to processing of each payroll for payment to verify that manual bank detail changes are supported by appropriate evidence and independently reviewed. See also recommendation M3(ii).	(i) MyView will continue to be promoted as the primary and preferred method for employees to add or amend their bank account details. A review will be undertaken to identify recurring issues that may prevent employees from accessing or using MyView, with actions taken where possible to address these issues and reduce reliance on manual bank mandate processes. (ii) A formal process will be implemented and communicated to the Payroll team to ensure that where bank details are transferred from one payroll record to another, the transfer is independently reviewed and evidenced. This check will confirm that the bank details have been transferred accurately and that the amendment has been completed in line with the agreed process. Evidence of the review will be retained to provide a clear audit trail. (iii) A formal process is already in place to ensure that manual bank detail changes are supported by appropriate evidence and	Operations Manager (Payroll)/ Payroll & HR Transactions Manager	30/11/26

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	Target Date
				subject to independent review. However, in response to the recommendation arising from the Systems Weaknesses Report, the current process will be reviewed to assess whether a system-based approval workflow can be introduced for manual bank mandates. This would further strengthen existing controls by providing systematic evidence of review and approval by a suitably authorised officer.		
H2	High	Testing of 20 timesheet and overtime claims found that multiple versions of claims forms were in use, authorisation practices were inconsistent, with approvals evidenced through a mixture of signed forms, emails and copied email recipients, and in some cases no evidence of approval was available. 18 of the 20 claims reviewed had been processed accurately; however, 1 overpayment (£797.20) and 1 underpayment (£116.51) were identified, demonstrating the risk of errors with the largely manual process.	Pending implementation of longer-term process improvements identified as a result of recommendation M2, the following measures should be introduced: (i) Authorisation standards for payroll claim forms should be established, formally agreed and documented. This should define acceptable methods of approval. Temporary arrangements (established in response to Covid) where managers were copied into submission emails as evidence of approval should be rescinded as these provide less assurance that claims have been actively	(i) The procedure notes currently held within Payroll will be reviewed in full and updated and circulated to the services to ensure that it accurately reflects current processes and guidance. (ii) In addition to circulating the updated document, we will take a proactive approach to raising awareness and reinforcing the process through a number of communication channels. The updated guidance will be highlighted during payroll briefing sessions, promoted on our Viva Engage page, included within the monthly Payroll newsletter, and	Operations Manager (Payroll) Payroll & HR Transactions Manager	30/11/26 30/11/26

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	Target Date
			reviewed and approved prior to processing. (ii) Procedures and guidance should be updated to reflect the approved authorisation and processing requirements and communicated to Payroll staff. All services submitting payroll claims should also be informed of the requirements to support consistent compliance with established controls. (iii) A risk-based quality assurance review of manually processed claims (for example, sample checking, targeted review of high-value claims, or periodic supervisory checks) should be introduced.	shared via Staff Connections. (iii) A 10% sample check of teachers' supply timesheets is currently undertaken as a quality assurance control to verify the accuracy of claims processed for payment. Due to the volume of timesheets received each pay period and the staffing resources available, it is not operationally feasible for Payroll to undertake detailed verification checks on every timesheet submitted. As a result, there is very limited capacity within the payroll processing timetable to introduce additional checking stages. (iv) A new electronic form will be developed incorporating a workflow process that routes submissions directly to the relevant Head Teacher for approval. The form will include a mandatory authorisation stage and will not progress to Payroll for processing until Head Teacher approval has been provided. The Workforce Planning Team will work in partnership with ICT to design and implement the form and will engage with Payroll to ensure that the information captured meets	Strategic Lead (Resources), Integrated People Services Workforce Planning and Staffing Manager, Integrated People Services Pay & HR Transactions Manager	Complete 01/09/27

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	Target Date
				operational and processing requirements. (v) The form will be designed with appropriate validation and control measures to minimise the risk of errors and improve the accuracy and efficiency of the process. (vi) Workforce Planning and Payroll will explore, in conjunction with ICT Services, the feasibility of uploading authorised claimed hours directly into the payroll system. This would reduce the current requirement for duplicate data handling and minimise the risk of manual processing errors. (vii) The proposed enhancement represents a significant programme of work and will require careful design, development, testing, and phased implementation across the service to ensure it is delivered effectively and without disruption to payment arrangements for supply/ relief staff. (viii) Guidance will be updated and circulated to reflect any agreed change in process to all stakeholders. In the meantime, Workforce Planning will provide	Workforce Planning Manager Payroll Operations Manager Workforce Planning Manager Payroll Operations Manager	01/01/27 01/01/27

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	Target Date
				reminder guidance on how the forms should be authorised. (ix) A review of the current form to be used will be undertaken to ensure that the forms are accurate and capture all required information. The new versions will then be circulated to all supply/ relief staff on the current list as well as Head Teachers indicating that only the current version of the form will be accepted from an agreed date going forward.		
M1	Medium	The SUPERVISOR profile provided unrestricted access to all payroll processing functions and was assigned to both internal and external support staff. Although mitigating controls were in place, there was no formal monitoring of activity undertaken using these accounts to provide assurance that access was being used only for authorised purposes.	(i) A periodic review of all users holding SUPERVISOR and PAYOFF access profiles should be conducted to provide assurance that access rights remain appropriate, proportionate to job responsibilities, and justified by an ongoing business requirement. (ii) A process should be established to monitor activity undertaken by users with SUPERVISOR access profiles, including periodic review of system activity logs, to provide assurance that access rights are being used appropriately and only for authorised purposes.	(i) Reviews of user access profiles are already undertaken jointly by Payroll and ICT to ensure that access rights remain appropriate to individuals' roles and business requirements. These arrangements will be expanded to include periodic reviews of all users holding SUPERVISOR access profiles, with ICT responsible for undertaking and documenting the reviews to provide assurance that access remains appropriate and supported by a valid business need.	Operations Manager (Payroll)/ Payroll & HR Transactions Manager/ Senior Applications Analyst	Complete

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	**Target Date**
			(iii) On completion of the apprenticeship/ training programme (or at key training milestones), access rights should be formally reviewed and revised, where necessary, to ensure access remains appropriate to the individual's role and responsibilities.	(ii) A formal process for monitoring the use of SUPERVISOR access profiles will be implemented. This will include periodic review of system activity logs, documented evidence of review, and investigation of any unusual, inappropriate, or unauthorised activity to provide assurance that elevated access rights are being used only for authorised business purposes. (iii) Upon completion of apprenticeship or training programmes, or at key training milestones, access rights will be reviewed. Any amendments required to ensure access remains aligned to the individual's role and responsibilities will be actioned through ICT's user access process.	Senior Applications Analyst Operations Manager (Payroll)/ Payroll & HR Transactions Manager	30/11/26 Complete
M2	Medium	The timesheet and overtime process involved multiple manual stages and relied primarily on managerial scrutiny to ensure accuracy, with budget holder monitoring providing a secondary detective control.	A review of the current timesheet and overtime process should be undertaken to identify opportunities to streamline manual steps and introduce proportionate system-based controls (e.g. electronic submission and validation), in order to improve efficiency and reduce the risk of errors arising from manual input and processing.	Currently, the automation of timesheet processing between MyView and ResourceLink does not form part of the scope of the HRP Project. However, from a Payroll perspective, the introduction of a system-based solution for timesheet submission, approval and transfer would deliver significant	Operations Manager (Payroll)/ Payroll & HR Transactions Manager	30/09/27

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	Target Date
				operational and governance benefits across the organisation. The implementation of a workforce management solution has been identified as a post-project deliverable and will be revisited following project completion.		
M3	Medium	Exception reports were generated for each payroll run and testing confirmed that identified exceptions had been reviewed and actioned by Payroll. However, in 1 case the review and check were completed by the same officer, and in another evidence of supervisory review was unclear. Weekly RL audit logs were generated but not reviewed, and although an enhanced audit reporting tool had been procured, it had not been implemented.	Management should formalise and strengthen the review and monitoring controls surrounding payroll exception reporting and system activity by: (i) Introducing independent review and sign-off of exception reports, ensuring that the officer performing the checks is not the same individual confirming completion. (ii) Implementing a routine (e.g. prior to processing of each payroll for payment) review of audit logs, focusing on high-risk changes such as amendments to pay, bank details, and employee records. (iii) Along with ICT Application Development, explore the use of the enhanced reporting module to support the audit log review process.	(i) Payroll calculation exceptions are currently reviewed and actioned by the Payroll Officer processing the payroll, with any required amendments recorded on the relevant exception reports. To strengthen the existing control environment, Payroll will introduce a programme of spot checks on exceptions where amendments have been made. These checks will be undertaken by a second Payroll Officer prior to the payroll progressing to BACS. A checking field will be added to the relevant exception report tabs to record completion of the secondary review and provide an audit trail of the checks undertaken. (ii) Payroll and ICT Application Development will work collaboratively to explore opportunities to enhance system reporting	Operations Manager (Payroll)/ Payroll & HR Transactions Manager Operations Manager (Payroll)/ Payroll & HR Transactions Manager/ Senior	31/12/26 31/12/26

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	Target Date
				functionality in support of the audit log review process. It is understood that work is already being progressed through the HRP project to deliver enhanced reporting capabilities, making amendments to employee records and other high-risk changes easier to identify, monitor and review. (iii) ICT Application Development will lead on the technical development of reporting solutions, while Payroll will provide operational expertise, define business requirements, and support testing and implementation to ensure the reporting meets operational and assurance needs.	Applications Analyst Operations Manager (Payroll)/ Payroll & HR Transactions Manager/ Senior Applications Analyst	31/12/26
L1	Low	There were minor weaknesses in the consistency of how Payroll recorded the checks undertaken to confirm that pay award updates had been correctly applied in RL across all pay and grading structures.	Checks should be undertaken to verify that pay award updates have been correctly applied across all pay and grading structures should be consistently recorded.	The Operations Managers will work collaboratively to develop a series of standardised payroll tables and checklists to support the implementation of future Pay Awards. The checklists will clearly outline responsibilities, critical milestones, validation requirements and sign-off points.	Operations Manager (Payroll)/ Payroll & HR Transactions Manager	30/11/26
L2	Low	The Corporate Cluster Business Continuity Plan (June 2025) covered key payroll processes, including backup, recovery and	The current Corporate Cluster BCP review process should be finalised, and the updated plan formally approved by the	BCP arrangements are overseen by the Chief Officer – Revenues & Commercialisation, who has delegated authority from the	CO Revenues & Commercialisation, Strategic Lead (Corporate	11/12/26

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	Target Date
		contingency arrangements, and was subject to scenario testing in February and June 2026. However, the plan remained under review and there was no clear evidence of formal approval.	Assistant Chief Executive – Corporate.	Assistant Chief Executive – Corporate in relation to this area. The suggested changes proposed by the Chief Officer – HR & Communications, Payroll & HR Transactions Manager and Strategic Lead – HR have been agreed and are currently awaiting final approval alongside the wider Corporate Cluster Business Continuity Plan.	Support)	

Control Weaknesses Report

Corporate

Payroll Bank Mandate Fraud

Description	Priority	No.
Major issues that managers need to address as a matter of urgency.	High	2
Important issues that managers should address and will benefit the Organisation if implemented.	Medium	0
Minor issues that are not critical but managers should address.	Low	0

Distribution:
Assistant Chief Executive – Corporate
Chief Officer – HR & Communications
Strategic Lead – HR
Pay & HR Transactions Manager

Audit Opinion

The opinion is based upon, and limited to, the work performed in respect of the subject under review. Internal Audit cannot provide total assurance that control weaknesses or irregularities do not exist. It is the opinion that **Limited Assurance** can be given in that weaknesses in the system of controls are such as to put the system objectives at risk, and/ or the level of non-compliance puts the system objectives at risk.

Report Ref: IF.3.6.25
Draft Date 06/08/26
Final Date: 29/09/26

1. Introduction

1.1 On 26 September 2025, the Corporate Fraud Team received notification from Payroll Management and the Corporate Information Governance Manager regarding a payroll mandate fraud and associated data breach. A fraudster had impersonated a Council employee, resulting in a salary payment £3,321.41 being redirected to a fraudulent bank account.

1.2 The Corporate Fraud Team undertook an immediate investigation to:

- Coordinate any immediate mitigating actions
- Establish the timeline of events
- Identify the method and nature of the fraud.

As part of the investigation, the internal control framework relating to payroll bank detail changes was reviewed to identify any control weaknesses and to implement immediate mitigating actions. A separate Internal Audit of Payroll has recently been undertaken and the control environment surrounding this fraud has been considered when carrying out that review. As part of this Payroll audit the effectiveness of internal controls and segregation of duties, focusing on system access, approval arrangements for sensitive changes, and the monitoring of exception reports and audit logs was considered. Therefore, a number of recommendations have been addressed within the separate payroll audit report.

2. Main findings

2.1 Summary of Fraud

On 1 September 2025, a phishing campaign targeted 12 Highland schools using emails impersonating teaching staff requesting payroll bank account changes. Most were quarantined; however, one email reached a Business Support Officer who correctly identified the request and advised the sender to submit it through MyView, the Council's secure employee self-service system. When the sender claimed they could not access MyView, they were provided with the generic payroll email address.

A subsequent email was received by Payroll requesting a bank detail change. Payroll advised the sender to use MyView but did not verify the sender's email address against the payroll records. The sender later claimed to be experiencing technical difficulties and requested a manual process to change bank details instead. Multiple urgent requests were submitted within a short period, which could have been recognised as 'red flags' of potentially fraudulent activity. Payroll issued a blank bank mandate form, which was completed and returned by the fraudster.

The fraudster subsequently requested copies of recent payslips. Two payslips were emailed by Payroll to the fraudster without any identity verification being undertaken. This resulted in the unauthorised disclosure of personal and financial information which is a reportable data breach.

The completed bank mandate form contained several anomalies:

- The employee tax code was entered where the payroll reference should have been.
- The address provided did not match payroll records.
- The bank information contained inconsistencies.
- The bank address provided did not correspond with the named bank.

These discrepancies were not identified at the time of processing. Payroll updated both the employee's address and bank details on the payroll system and subsequently confirmed to the fraudster that the changes would take effect for the September payroll.

On 26 September 2025, the genuine employee contacted Payroll after failing to receive their salary payment. This

was investigated by Payroll which identified that the salary payment had been redirected to a different bank account.

Payroll Management immediately identified the fraudulent amendment, notified the affected employee, arranged a replacement payment for the employee, reported the data breach to the Corporate Information Governance Manager (Data Protection Officer), reported the matter to ICT and the bank and suspended manual bank mandate processing pending investigation.

The fraud was initially reported to Police Scotland by the Employee. The Corporate Fraud Team subsequently provided information and a statement to Police Scotland. Police Scotland carried out enquiries resulting in the case being subsequently closed and recorded as an 'undetected crime' on 10 February 2026.

2.2 Control weaknesses identified

As a result of the fraud several control weaknesses were identified. The following provides a high-level summary of where improvements in processes and procedures are required.

I. There were indicators that may have suggested fraudulent activity (e.g. not using MyView, urgency, external email addresses and repeated requests for bank changes). Enhancing fraud awareness, encouraging professional scepticism and providing targeted refresher training would better equip staff involved in payroll processing to identify such 'red flags' at an early stage and help prevent fraudulent payments. (See action plan H1).

II. At the time of the incident, no formal written procedures existed for processing manual bank mandate changes. Processing changes to employee payroll bank account details relied on payroll staff following a verbal procedure guided by training and local practice. In this instance the stated verbal procedure was not followed. This has been rectified with a procedure note put in place immediately following the incident and communicated to payroll staff.

III. Continued use of manual bank account change processes. Although employees can securely add and amend their bank account details through MyView, manual bank mandate forms were routinely processed reducing efficiency and further increasing fraud risk exposure. (Further addressed in the Payroll Internal Audit Report).

IV. Lack of system based enforced segregation of duties, a single Payroll Officer could, receive requests and amend payroll standing data (bank details) without independent review or approval. A compensating control requiring supervisory review of all bank detail changes was put in place immediately following the incident. However, its effectiveness depends on consistent review and timely follow-up of exceptions to identify and address instances of non-compliance. (Further addressed in the Payroll Internal Audit Report and see action plan H2)

V. Weak identity verification controls. The manual request was processed without independent verification of the requestor's identity or validation of bank account information provided. This was contrary to the stated verbal procedure. This has been rectified with a procedure put in place immediately following the incident. (Further addressed in the Payroll Internal Audit Report).

VI. Inadequate supervisory oversight. A comprehensive management review of all changes to bank details was not performed, as no exception reporting was in place to identify changes and facilitate review. Audit logging functionality existed but was not known about by Payroll staff and therefore not used to monitor or

review high-risk amendments. Payroll management now have access to audit logs to enable monitoring and supervisory review of all bank detail changes. This was put in place in place following the incident. (Further addressed in the Payroll Internal Audit Report).

VII. Data Protection Breach. Two payslips containing personal information were disclosed to the fraudster. Employees have access to their payslips through MyView. Payroll staff should only refer employees to MyView to access their payslips. Immediately following the incident Payroll staff have been instructed not to share employee payslips via email.

3. Conclusion

3.1 The investigation identified weaknesses in the operation of the payroll bank mandate change process. These weaknesses directly contributed to:

- The diversion of £3,321.41 in salary payment to a fraudster.
- The unauthorised disclosure of an employee's personal data to the fraudster.

3.2 Management acted promptly once the fraud was identified by suspending manual processing, supporting the affected employee and initiating recovery actions. However, the control framework operating at the time of the incident was insufficient to prevent or detect the fraud.

3.3 The implementation of strengthened procedures, verification controls, improved management oversight, and increased cyber security awareness will be essential to mitigating the risk of a similar incident occurring in the future.

4. Action Plan

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	**Target Date**
H1	High	Fraud awareness training requires improvement to better equip staff involved in payroll processing to identify early 'red flags' which could help prevent fraudulent payments.	Fraud awareness training should be enhanced for all staff involved in payroll processing, with a particular focus on recognising common 'red flags' associated with bank mandate fraud, such as changes to bank details, email anomalies, and urgent or unusual requests. Strengthening staff awareness in this area will improve early identification of suspicious activity and help prevent fraudulent payments.	Payroll will work with Learning & Development (L&D) to develop a fraud awareness presentation and training video based on a real-life case study. The training will be mandatory for all relevant employees and will aim to increase awareness of fraud risks, prevention measures, and organisational responsibilities. Knowledge, processes, and best practices identified through discussions with Creditors will be incorporated where appropriate. In addition, all relevant staff will be required to complete the Cyber Security Awareness training course, which covers the identification and prevention of phishing attacks.	Payroll Operations Manager/ Payroll & HR Transactions Manager	30/11/26
H2	High	Lack of segregation of duties, a single member of staff can input, amend and authorise amendments to bank details. There were no routine supervisory checks to verify bank detail changes made ahead of payroll processing. Audit logging functionality existed but was not known by Payroll staff and therefore not used to monitor or review bank detail amendments.	System-based controls should be implemented to enforce segregation of duties to ensure that a single person cannot input, amend and authorise amendments to bank details. Management should engage with the payroll system provider to identify and implement a technical solution to enforce segregation of duties for changes to bank account details. This will strengthen control effectiveness by ensuring that all bank detail amendments are	A review of the controls currently available within the payroll system will be undertaken with the system provider, Zellis, to determine whether a system-based approval workflow can be implemented for manual bank mandate changes. A call has been logged with Zellis to investigate the feasibility of introducing a technical solution whereby any manually entered or amended bank details must be independently authorised by	Payroll Operations Manager/ Payroll & HR Transactions Manager	30/11/26

Ref	Priority	Finding	Recommendation	Management Response	Implementation	
					Responsible Officer	**Target Date**
			reviewed by a second person reducing the risk of unauthorised or inappropriate payroll transactions.	a superior before payments can be processed using those details. In addition, the manual bank mandate form has recently been enhanced to include a security check requiring existing employees requesting a bank account change to provide their previous bank account details. This mirrors the verification process used within MyView and provides additional assurance that amendment requests are genuine. Should a system-based solution be available, Payroll will work with Zellis and ICT to incorporate the control into business processes. While a system solution is not currently available, Payroll operates manual checking procedures whereby bank detail changes are independently reviewed and verified by a senior member of staff before payroll is finalised.		