NORTH AYRSHIRE COUNCIL

1 June 2021

Audit and Scrutiny Committee

Title:	**Internal Audit Reports issued**
Purpose:	To inform the Committee of the findings of Internal Audit work completed during March and April 2021.
Recommendation:	That the Committee considers the outcomes from the Internal Audit work completed.

1. Executive Summary

1.1 The Council's local Code of Corporate Governance requires effective arrangements to be put in place for the objective review of risk management and internal control. Internal Audit is an important element in this framework as it reviews internal controls and offers Elected Members and officers an objective and independent appraisal of how effectively resources are being managed.

1.2 The remit of the Audit and Scrutiny Committee includes the monitoring of Internal Audit activity. The submission and consideration of regular reports assists the Committee in fulfilling this remit.

2. Background

2.1 This report provides information on Internal Audit work completed during March and April 2021. Internal control reviews have been completed in respect of the areas detailed in Appendix 1 to this report. The aim of these reviews is to provide assurance that the internal control framework within the areas examined is appropriate and operating effectively.

2.2 The findings from each audit assignment have been notified in writing to the Chief Executive, the Section 95 Officer and the relevant Executive Director and Head of Service on the completion of each assignment. Where appropriate, this has included an action plan with recommendations for improving internal control. Appendix 1 includes the report and action plan from each audit.

2.3 The findings from 8 separate audit assignments are detailed at Appendix 1 to this report and the levels of assurance for each are noted in the table below:

Audit Title	**Assurance Level**
Parent Pay system	Limited
Internet and email controls	Reasonable
Information Governance and Data Protection	Reasonable
Accounts Receivable	Reasonable
Accounts Payable Transaction Testing Q4	Reasonable
Payroll Transaction Testing Q3	Reasonable
Allowances and Pay adjustments	Substantial
HRA Planned Maintenance and Reactive Repairs	Substantial

2.4 The key findings are as follows:

- There is an absence of any written procedures for users of the Parent Pay system, both in Facilities Management and Education
- The Service did not complete a Data Protection Impact Assessment, Data Sharing Agreement or IT, Cyber and Information Security Schedule when the Parent Pay system was procured, although it recognised that it is now in the process of being replaced.
- It was identified that there is no process in place for removing access to shared electronic mailboxes when an employee moves jobs.

3. Proposals

3.1 It is proposed that the Committee considers the outcomes from the Internal Audit work completed during March and April 2021.

4. Implications/Socio-economic Duty

Financial

4.1 None.

Human Resources

4.2 None.

Legal

4.3 None.

Equality/Socio-economic

4.4 None.

Environmental and Sustainability

4.5 None.

Key Priorities

4.6 The work of Internal Audit helps to support the efficient delivery of the strategic priorities within the Council Plan 2019-2024.

Community Wealth Building

4.7 None.

5. Consultation

5.1 The relevant Services are consulted on Internal Audit findings during each audit assignment.

Mark Boyd
Head of Service (Finance)

For further information please contact **Paul Doak, Senior Manager (Audit, Fraud, Safety and Insurance),** on **01294-324561**.

Background Papers
None.

FACILITIES MANAGEMENT PARENTPAY SYSTEM

1 Background

1.1 Facilities Management (FM) have been working towards cashless school meals across all Council schools since 2017/18, with ParentPay being the software used to facilitate this.

1.2 The risk of handling cash during the coronavirus pandemic resulted in Facilities Management accelerating the rollout of ParentPay, meaning all schools are now cashless in terms of school meals.

2 Objectives and Scope

2.1 The objective of this audit was to ensure that:-

- Written procedures exist to support staff using ParentPay
- Personal data within ParentPay is secure
- Checks are in place to confirm that all cash payable to the Council is received
- Debt is being managed effectively

3 Findings

Procedures

3.1 FM are the owners of ParentPay, however Education are key users of the system, therefore procedures were requested from both Services.

3.2 Neither Service has written procedures to cover the processes that their staff are responsible for undertaking within ParentPay. Both Services were aware of this shortfall and were considering their production prior to this audit. **(action point a)**

3.3 Whilst no written procedures are currently available, both Services have confirmed that staff using ParentPay have had basic training relevant to their role.

Data Security

3.4 ParentPay have recently provided the Council with a detailed statement on how they guard against information security and cyber threats. This statement was reviewed and found to be satisfactory by Audit.

3.5 During the tendering and award of the contract to ParentPay, the following data security documents should have been completed:

- Data Protection Impact Assessment (DPIA)
- Data Sharing Agreement
- IT, Cyber and Information Security Schedule

3.6 A DPIA has not been completed for ParentPay, therefore Audit have requested that FM prepare one **(action point b).**

3.7 ParentPay provided the Council with a data sharing agreement as part of the contract award. Audit were unable to gain assurance that the agreement was reviewed by IT or Legal prior to signing, therefore could not confirm that the terms are fair and reasonable for the Council **(action point c).**

3.8 Corporate Procurement were unable to find evidence of an IT, Cyber and Information Security Schedule having been completed during the contract award **(action point d)**.

Council Income

3.9 PARIS (the Council's cash management system) is used to upload income information received from ParentPay. A file is then created to update the ledger.

3.10 Both the transfer of data from PARIS into the general ledger, and the reconciliation of the Council's bank accounts have been covered in previous audits, with no significant issues noted. As a result, no further testing has been undertaken as part of this audit.

Debt Recovery

3.11 As at October 2020, there was approximately £220k of debt relating to unpaid school meals. FM intend to write off £32k of this debt as it relates to pupils who have now been granted free school meals. In addition, it is hoped that once Corporate Debt Recovery resume pursuing debt (which has currently been paused due to coronavirus) the overall debt figure will be further reduced.

3.12 FM are proactively looking at ways to reduce debt levels, with a focus of minimising the occurrence of debt in the first place. A more joined up approach between FM, Education and Customer Services has been proposed as part of the solution.

3.13 Once a revised approach to minimising school meal debt is agreed, detailed procedures should be included as part of the overall ParentPay procedures **(action a).**

4 Internal Audit Opinion

4.1 Overall, limited assurance was obtained with regard to the controls surrounding the ParentPay system.

4.2 Procedures provide guidance to staff in terms of their role and responsibilities. A lack of written guidance increases the risk of error and inconsistencies when using the system.

Definitions of Assurance Levels:

Substantial	The framework of governance, risk management and control is adequate and effective.
Reasonable	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
None	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

NB The level of assurance given is at the discretion of Internal Audit.

KEY FINDINGS AND ACTION PLAN
FACILITIES MANAGEMENT PARENTPAY SYSTEM

Action	a(1)
Finding	Written procedures are not available for users of ParentPay
Action Description	Detailed written procedures should be completed. As system owners, Facilities Management should ensure these cover the administrative side of the software.
Risk	Errors are made due to a lack of written guidance for ParentPay users; inconsistent approach when dealing with pupil debt
Priority (1, 2, 3)	2
Paragraph Reference	3.2, 3.13
Managed by	Yvonne Baulk, Head of Service (Physical Environment)
Assigned to	Neil McAleese
Due Date	31 May 2021
Management Comment	FM will prepare procedures for all FM related processes.

Action	a(2)
Finding	Written procedures are not available for users of ParentPay
Action Description	Detailed written procedures should be completed for system users within Education.
Risk	Errors are made due to a lack of written guidance for ParentPay users; inconsistent approach when dealing with pupil debt
Priority (1, 2, 3)	2
Paragraph Reference	3.2, 3.13
Managed by	Andrew McClelland, Head of Service (Education)
Assigned to	Lynn Taylor
Due Date	31 May 2021
Management Comment	A procedures document will be produced for both school-based staff and parents/carers.

Action	b
Finding	A Data Protection Impact Assessment has not been completed.
Action Description	A Data Protection Impact Assessment document should be prepared. This document is a 'live' document and therefore should continue to be updated for any process changes or new risks.
Risk	Personal data is at risk of misuse; Council reputation damage; Council could be fined by the Information Commissioner's Office
Priority (1, 2, 3)	1
Paragraph Reference	3.6
Managed by	Yvonne Baulk, Head of Service (Physical Environment)
Assigned to	Neil McAleese
Due Date	Completed
Management Comment	DPIA has be prepared and will be monitored as required.

Action	c
Finding	Audit were unable to confirm that the Data Sharing Agreement which has been signed on behalf of the Council was confirmed as fair and reasonable by IT or Legal prior to signing.
Action Description	The Data Sharing Agreement with ParentPay should be reviewed by IT and Legal to confirm that it is fair and reasonable. Any issues should be immediately raised and negotiated with ParentPay.
Risk	The Council has signed an unfavourable legal document which could have ramifications should a data breach occur; Personal data is at risk of misuse; Council reputation damage; Council could be fined by the Information Commissioner's Office
Priority (1, 2, 3)	1
Paragraph Reference	3.7
Managed by	N/A
Assigned to	N/A
Due Date	N/A
Management Comment	Agreed with Audit that this is no longer required as the contract is almost at an end and the Council is bound by the current agreement.

Action	d
Finding	IT, Cyber and Information Security Schedule hasn't been completed.
Action Description	An IT, Cyber and Information Security Schedule should be prepared.
Risk	Personal data is at risk of misuse; Council reputation damage; Council could be fined by the Information Commissioner's Office
Priority (1, 2, 3)	1
Paragraph Reference	3.8
Managed by	Yvonne Baulk, Head of Service (Physical Environment)
Assigned to	Neil McAleese
Due Date	N/A
Management Comment	Facilities Management recognise that this process was not documented previously but confirm that steps have been taken to remediate this as part of the tender process for a new online payments supplier.

Priority Key used in Action Plan

1 (High)	Control weakness where there is a material impact on the achievement of the control objectives, generally requiring prompt attention.
2 (Medium)	Control weakness which needs to be rectified, but where there is no material impact on the achievement of the control objectives.
3 (Low)	Minor weakness or points for improvement.

INTERNET AND EMAIL CONTROLS

1 Background

1.1 The introduction of Office 365 is in line with a key objective of the Council's Digital Strategy. Office 365 is a cloud-based approach to business application delivery.

1.2 Part of the Office 365 project was to migrate the Council's existing Lotus Notes environment to Exchange Online, which has been fully implemented. This audit focuses on the security controls surrounding Exchange Online although it should be noted that some controls relate to Office 365 as a whole.

1.3 IT Services are responsible for the administration of Exchange Online.

2 Objectives and Scope

2.1 The main objectives of the audit were to ensure that:

- security roles and responsibilities have been identified and are managed with the service provider and relevant policy requirements are being met.
- access to privileged accounts is appropriately restricted, email logs are available, users access controls are appropriate and access to shared mailboxes is properly controlled.
- adequate security controls are in place to protect our data and monitoring is in place to detect unusual activity.
- appropriate malware prevention controls are in place to protect the network from malicious content.
- email access on tablets and mobile phones is secure, controlled and covered by policy.

3 Findings

Contract Compliance and Policy Requirements

3.1 The email retention policy was agreed by the project board in May 2020 and approved by Executive Leadership Team (ELT) in December 2020; however, it has not yet been implemented on Exchange Online. Information Governance will advise IT Services to go live with this policy after a corporate communication has been issued to staff. **(action a)**

3.2 Microsoft provides a resilient environment to ensure the Council retains access to emails and can recover emails within 30 days of deletion. For emails deleted after 30 days, there is currently no way to recover such emails. IT Services advised they have a capital funding bid of £150,000 for a new backup and recovery system to deal with this. The Capital Investment Programme was approved by the Council on Thursday 4th March 2021.

Review of Exchange Admin Roles and Controls around Email Accounts

3.3 Microsoft recommends between 2 and 4 global administrators as this role has almost unlimited access to the Council's settings and most of the data within Office 365 and therefore provides a security threat. The Council exceeds this recommendation as there are 6 global administrators that all work in IT Services. IT Services reviewed this access and confirmed this access is appropriate and necessary to allow the Operations team to carry out their job as well as to provide cover and continuity. To protect this level of access, multi-factor authentication was implemented in 2020 to minimise the risk of unauthorised access. IT Services will keep the security and access to global accounts under review.

3.4 Microsoft also recommends assigning the least permissive role. The auditor reviewed the users with Exchange admin role. Initially this was restricted to 6 relevant IT Services staff, but this was changed during the audit to 20 IT Services staff. This is to allow the Customer Team to apply out of office for people who go off suddenly and there is currently no individual way of giving them that ability without the full Exchange admin role. This was raised with the Senior Manager who requested this was reduced. IT have confirmed this has now been reduced to 5 relevant IT users.

3.5 The auditor tested for leavers who still have an active email account. There were 3,222 email accounts and 110 of them were for employees who had left. Of these 110 employees, 22 employees left in 2019 or earlier and the rest left in 2020. IT reviewed the results and confirmed that the leavers process disabled the active directory account and changed the individual user email account to a shared mailbox so there is no risk of unauthorised access.

3.6 Microsoft recommends blocking sign in for the accounts associated with a shared mailbox to prevent an admin user resetting the password on such accounts. This also prevents an attacker gaining access to the shared mailbox credentials to allow the user account to log in to the shared mailbox and send email. IT Services confirmed this is being done for new shared mailboxes set up in Exchange Online but has not been implemented for existing shared mailboxes migrated from Lotus Notes. This was rectified during the audit.

3.7 The auditor selected a sample of 10 shared mailboxes that are at a higher risk of sending and receiving sensitive data as per the title of the mailbox. This testing identified 5 employees that no longer work for the team using the shared mailbox but still have access to it. The Information Management Officer in Information Governance is not aware of any guidance advising staff to review and update access to shared and group mailboxes. There is also no process in place for ensure shared mailboxes are reviewed periodically and updated on a timely basis. **(action b)**

Email Security Controls

3.8 IT Services has no process in place to review the 'Third-Party Vulnerability Assessment of Office 365' annual report made available by Microsoft to determine if any action is required to be taken by the Council to tighten the security of our Office 365 environment. **(action c)**

Malware Prevention

3.9 The Council utilises Exchange Online Protection, which is the cloud-based filtering service that helps protect the Council against spam and malware. Suspicious or infected malicious objects are quarantined. This is controlled via the Exchange admin centre and access to this is restricted to key IT Services staff. There are no findings to report from this testing.

Email on Mobile Devices

3.10 The Bring Your Own Device (BYOD) policy, and additional guidance referred to in the draft version, has not yet been agreed and issued. **(action d)**

3.11 Microsoft Intune is used for Mobile Device Management. Access to this is restricted to a small number of IT staff. The auditor compared the security configuration settings as per the draft BYOD policy to the security configuration settings as per the different device enrolment policies set up. This comparison identified differences in the security configurations for each type of device so there is no standard approach. It should be noted that all requires a password and provides a minimum password length of 4. The specific discrepancies have been passed to IT to consider when finalising the BYOD policy. **(action e)**

4 Internal Audit Opinion

4.1 Overall, reasonable assurance was obtained with regard to the security controls around Exchange Online. Implementation of the audit actions will help to tighten the security and controls in this area.

Definitions of Assurance Levels:

Substantial	The framework of governance, risk management and control is adequate and effective.
Reasonable	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
None	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

NB The level of assurance given is at the discretion of Internal Audit.

KEY FINDINGS AND ACTION PLAN
INTERNET AND EMAIL CONTROLS

Action	a
Finding	The email retention policy was agreed by the project board in May 2020 and approved by ELT in December 2020; however, it has not yet been implemented on Exchange Online. Information Governance will advise IT Services to go live with this policy after a corporate communication has been issued to staff.
Action Description	Information Governance should liaise with the project manager, issue the corporate communication, and advise IT to go live with the agreed policy.
Risk	Emails are retained longer than required resulting in a GDPR breach.
Priority (1, 2, 3)	2
Paragraph Reference	3.1
Managed by	Andrew Fraser, Head of Service (Democratic)
Assigned to	Lauren Lewis, Information Management Officer (Democratic)
Due Date	30/04/2021
Management Comment	- Article to be written for all staff to raise awareness of Email Retention Policy prior to IT switch on. Comms will be sent via News in Brief and O365 SharePoint site. - Supporting 'how to' video on how to save emails out of Outlook and into shared file repository (shared drive/SharePoint/OneDrive) will be saved to O365 SharePoint site for all staff to view. - Email Retention Policy can then be switched on by IT.

Action	b
Finding	Audit testing identified a number of employees that still have access to a shared mailbox despite moving jobs. The Information Management Officer in Information Governance is not aware of any guidance advising staff to review and update access to shared and group mailboxes. There is also no process in place for ensure shared mailboxes are reviewed periodically and updated on a timely basis.
Action Description	Information Governance and IT Services should work together to introduce a process for reviewing and updating who has access to shared mailboxes and group mailboxes.
Risk	Inappropriate access to personal and sensitive data.
Priority (1, 2, 3)	1
Paragraph Reference	3.7
Managed by	Andrew Fraser, Head of Service (Democratic) Fiona Walker, Head of Service (People and ICT)
Assigned to	Alan Lindsay, Snr Tech Officer (IT Services) Lauren Lewis, Information Management Officer (Democratic)
Due Date	31/12/2021
Management Comment	IT Services will work with Information Governance to introduce a process for reviewing and updating who has access to shared mailboxes and group mailboxes. This is likely to include looking at commercial software solutions that could support this.

	Consideration and then selection of the right solution will take several months and may have budgetary implications if it is deemed that a commercial 'off the shelf' solution is required. Information Governance will draft corporate email guidance for staff and update relevant policies to highlight governance risks of outdated access controls for shared mailboxes.

Action	c
Finding	IT Services has no process in place to review the Third-Party Vulnerability Assessment of Office 365 annual report made available by Microsoft to determine if any action is required to be taken by the Council to tighten the security of our Office 365 environment.
Action Description	IT Services should ensure that they review the Third-Party Vulnerability Assessment of Office 365 annual report made available by Microsoft to determine if any action is required to be taken to tighten the security of our Office 365 environment.
Risk	Identified vulnerabilities are not rectified.
Priority (1, 2, 3)	2
Paragraph Reference	3.8
Managed by	Fiona Walker, Head of Service (People and ICT)
Assigned to	Derek Nelson, ICT & Cyber Security Architect
Due Date	31st July 2021
Management Comment	A review of the Third-Party Vulnerability Assessment of Office 365 annual report will be scheduled to occur annually on the 31st March with any subsequent actions noted in the cyber risk register and resolved as appropriate.

Action	d
Finding	The Bring Your Own Device (BYOD) policy, and additional guidance referred to in the draft version, has not yet been agreed and issued.
Action Description	The Bring Your Own Device policy and additional guidance should be finalised, agreed and issued.
Risk	Responsibilities of the Council and employees have not been defined, agreed and communicated.
Priority (1, 2, 3)	2
Paragraph Reference	3.10
Managed by	Fiona Walker, Head of Service (People and ICT)
Assigned to	Derek Nelson, ICT & Cyber Security Architect
Due Date	31st July 2021
Management Comment	Policy will be reviewed, updated where required, and distributed to all registered BYOD users.

Action	e
Finding	The comparison between the security configuration settings as per the draft BYOD policy and the settings as per the device enrolment policies identified differences in the security configurations for each type of device so there is no standard approach. It should be noted that all requires a password and provides a minimum password length of 4.
Action Description	Once the BYOD policy has been agreed, the security configuration settings as per the device enrolment policies should be reviewed and brought in line with the BYOD policy.
Risk	Inappropriate access to Council data and potential data loss.
Priority (1, 2, 3)	2
Paragraph Reference	3.11
Managed by	Fiona Walker, Head of Service (People and ICT)
Assigned to	Derek Nelson, ICT & Cyber Security Architect
Due Date	31st July 2021
Management Comment	The security configuration requirements will be aligned, where appropriate and possible, with the updated BYOD policy.

Priority Key used in Action Plan

1 (High)	Control weakness where there is a material impact on the achievement of the control objectives, generally requiring prompt attention.
2 (Medium)	Control weakness which needs to be rectified, but where there is no material impact on the achievement of the control objectives.
3 (Low)	Minor weakness or points for improvement.

INFORMATION GOVERNANCE AND DATA PROTECTION

1 Background

1.1 The EU General Data Protection Regulation (GDPR) became part of UK law in the Data Protection Act 2018.

1.2 The Information Governance team has undergone a number of changes in the last 2 years and the manager's post remains vacant. The Data Protection Officer role, which is a requirement of the GDPR, has been filled on an interim basis.

1.3 The Council previously had a network of service representatives for Data Protection issues, known as the Data Protection Advisory Group (DPAG). This group has been disbanded, and a replacement Corporate Information Governance Panel is in the process of being set up but has not yet met or set Terms of Reference.

1.4 As part of the audit, a survey was sent to representatives of Council Services. Responses were received from:

Chief Executive's Directorate – Member Services, Corporate Fraud Team, Financial Management, Insurance, Corporate Procurement, HR Operations, Organisational Development, Payroll, HR Resourcing, Customer Services, Transformation

Place – Employability and Skills, Protective Services, Housing

Communities – Education, Connected Communities

Health and Social Care Partnership (HSCP)

2 Objectives and Scope

2.1 The audit focussed on the implementation of GDPR requirements in relation to information sharing, privacy information and retention and disposal of records.

2.2 The main objectives of the audit were to ensure that the Council has:

- processes in place to fulfil individual's rights as defined in the GDPR.
- accountability arrangements in place in line with the GDPR.
- the necessary controls over records management, as required by the GDPR.

3 Findings

Individual Rights

3.1 The Council has an overarching privacy policy statement on its external website and a number of service-specific privacy notices. All the services who responded to the survey were taking steps to inform service users and other contacts of how the Council uses their data.

3.2 Services were asked if they produce privacy information tailored for children, but all of the respondents stated that they do not. However, from discussions with the Information Management Officer, it seems likely that some individual establishments and teams, particularly within Education and HSCP, are doing this, but the people completing the survey may have been unaware of that. It is important that the Council explains to children and young people what it does with their personal data in appropriate language. **(Action a)**

3.3 There is a corporate Record Retention Schedule which is dated 11th February 2010. There are also a number of service-specific schedules, most of which were last reviewed between June 2010 and February 2013. Updated Records Retention Schedules based upon the Scottish Council on Archives Records Retention Schedules (SCARRS) are being produced as an output of the data cleanse work being undertaken as part of the implementation of Office 365, which is moving the Council's data to Sharepoint. This work is already underway, but it is a very large project. The current expectation is that the retention schedules will be completed by mid to late 2023. As an interim measure, the old retention schedules could be removed from Connects and replaced with a link to SCARRS, upon which the new schedules will be based. **(Action b)**

3.4 The Northgate system used for Council Tax does not have archiving facilities and it is therefore necessary to keep data from prior years, in order to continue pursuing debts from those prior years. This has been noted in the Council's Information Asset Register with a recommendation that, when the system reaches the end of its lifecycle, the specification for any future system should require retention facilities which are compatible with GDPR requirements.

Accountability

3.5 The Council has a mandatory half-day training course on Information Governance, which includes information on information sharing. However, during the Covid-19 pandemic it has not been possible to run these courses. There is an e-learning course available to all employees, but it does not give guidance on information sharing. It includes a video on data handling, but this is out-of-date, referring to the previous information classification scheme and Navigate, the Council's intranet site prior to Connects. **(Action c)**

3.6 A sample of 5 contracts which involved sharing personal data was selected from the Council's contract register. In 4 cases suitable data sharing agreements were in place. In the 5th case, the relevant procurement officer is actively pursuing the contractor for the signed agreement.

3.7 The Council's Information Asset Register is an important tool in ensuring compliance with GDPR requirements. It identifies all the information assets held by the Council and information about each one, such as whether and how they are shared with other parties and whether they are processed outwith the European Economic Area. Services are prompted to review their entries on an annual basis. However, the database is built on a platform which has reached the end of its lifecycle and a replacement system will require to be purchased. **(Action d)**

3.8 The requirement to undertake Data Protection Impact Assessments (DPIAs) is built into the procurement process. Survey respondents were aware of the requirement to undertake DPIAs.

Records Management

3.9 There is guidance on records management on Connects, including a Records Management Manual which was updated in 2018.

3.10 There is advice regarding taking records offsite on Connects and in the face-to-face training mentioned at 3.5 above. As at 3.5, it would be beneficial to include more information on this in the e-learning course. Advice on looking after Council data while working from home was included in the June 2020 "Staff Talk" magazine in response to the increase in working from home during the Covid-19 pandemic. **(Action c)**

4 Internal Audit Opinion

4.1 Overall, reasonable assurance was obtained with regard to the implementation of GDPR requirements in relation to information sharing, privacy information and retention and disposal of records.

Definitions of Assurance Levels:

Substantial	The framework of governance, risk management and control is adequate and effective.
Reasonable	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
None	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

NB The level of assurance given is at the discretion of Internal Audit.

KEY FINDINGS AND ACTION PLAN
INFORMATION GOVERNANCE AND DATA PROTECTION

Action	a
Finding	Survey respondents stated that no privacy information specifically for children has been produced. In discussion with the Information Management Officer, it seems likely that some individual establishments and teams have produced such information, but that officers completing the survey were unaware of this.
Action Description	The Corporate Information Governance Group should review the privacy information produced for children and ensure that best practice is followed.
Risk	Children and young people do not receive appropriate information to make them aware of how their information is handled by the Council, leading to a potential breach of the GDPR. Information given to children and young people is inconsistent or not appropriately worded. Officer time is spent producing such information when examples of good practice already exist.
Priority (1, 2, 3)	2
Paragraph Reference	3.2
Managed by	Andrew Fraser, Head of Service (Democratic Services)
Assigned to	Lauren Lewis, Information Management Officer/Kirsty Hamilton, Data Protection Officer
Due Date	31/08/2021
Management Comment	Information Governance to liaise with relevant Services to identify key areas for focus – predominantly within HSCP and Education. Due date chosen to align with school term return. Evidence of privacy notices/information provided that is tailored to children will be attached to audit report to support compliance.

Action	b
Finding	The current record retention schedules are up to 10 years old. There is an ongoing project which will produce revised retention schedules, but these are not expected to be completed until 2023.
Action Description	Information Governance should consider removing the old retention schedules from Connects and replacing them with a link to the SCARRS as an interim measure until the new North Ayrshire Council records retention schedules are available.
Risk	Services are making decisions on how long to retain records based upon out-of-date information which could potentially include legislation which has been superseded.
Priority (1, 2, 3)	2
Paragraph Reference	3.3
Managed by	Andrew Fraser, Head of Service (Democratic Services)
Assigned to	Lauren Lewis, Information Management Officer
Due Date	30/04/2021
Management Comment	Access to the retention schedule will be retained by Records Management for reference as existing records will have retention applied as per this schedule for a number of years to come; however any records having retention applied from x date (tbc) will be retained according to SCARRS. This will be reflected in the wording on Connects.

Action	c
Finding	Although the mandatory Information Governance training course does cover data sharing and taking data offsite, it has not been possible to run the course during the Covid-19 pandemic. The e-learning available to officers does not cover data sharing in any depth and also includes out-of-date references.
Action Description	Information Governance should update the e-learning available to officers and ensure that it includes guidance on data sharing.
Risk	Officers do not receive suitable training on information sharing if they are unable to attend in-person training. They receive out-of-date information on Council policies and procedures.
Priority (1, 2, 3)	2
Paragraph Reference	3.5, 3.10
Managed by	Andrew Fraser, Head of Service (Democratic Services)
Assigned to	Kirsty Hamilton, Data Protection Officer
Due Date	31/05/2021
Management Comment	Content can be reviewed and scoped by Information Governance however the transfer of material to the online platform is reliant on HR L&OD. L&OD are in the process of migrating to a new online training platform and therefore due date may be subject to change based on resource within Service and go live date of the training system.

Action	d
Finding	The Information Asset Register database is built on a platform which has reached the end of its lifecycle and a replacement system will require to be purchased.
Action Description	Information Governance should procure a replacement database for the Information Asset Register.
Risk	The database, which is essential for GDPR compliance, ceases to be fit for purpose.
Priority (1, 2, 3)	2
Paragraph Reference	3.7
Managed by	Andrew Fraser, Head of Service (Democratic Services);
Assigned to	Kirsty Hamilton, Data Protection Officer
Due Date	31/03/2022
Management Comment	Discussions ongoing with IT to ensure a solution to current database issues is found. Ongoing support to the database will continue however no further updates will be made.

Priority Key used in Action Plan

1 (High)	Control weakness where there is a material impact on the achievement of the control objectives, generally requiring prompt attention.
2 (Medium)	Control weakness which needs to be rectified, but where there is no material impact on the achievement of the control objectives.
3 (Low)	Minor weakness or points for improvement.

ACCOUNTS RECEIVABLE

1 Background

1.1 North Ayrshire Council has a Sundry Debtors Policy which details the procedures to be followed when dealing with accounts receivable. All Services have the responsibility to recover as much of the income owed as possible.

1.2 The COVID-19 pandemic has had an impact on the issuing of invoices and collection of debtors' income.

2 Objectives and Scope

2.1 The main objectives of this audit were to ensure that: -

- there is an adequate control framework over access to and operation of the accounts receivable system
- debt is properly raised for all chargeable goods and services and recorded in the accounts receivable ledger in a consistent and timely manner and is complete, accurate and valid
- that all payments received from valid customers are promptly processed and accurately recorded in the accounts receivable ledger
- debt management, arrears follow up procedures and bad debt write offs are properly controlled
- the outputs from the accounts receivable ledger are complete, accurate and valid and are produced and reconciled in a consistent and appropriate format, in a timely manner

3 Findings

Control Framework

3.1 The Sundry Debt Policy was updated in 2019 and, together with Integra procedural instructions, is available to staff on Connects.

3.2 The debtor process is administered through Integra. Integra SLS (sales ledger system) access requests are made by the employee's line manager and administered by the Finance Team. Responsibility for managing access remains with the manager responsible for the employee.

3.3 Audit testing identified 2,921 employees had access to the system; of these 674 were non active leaving 2,247 active accounts. Of the active accounts 1,228 have never been accessed therefore not activating system security protocols.

3.4 A data matching exercise between the Sales Ledger current users and Council leavers, identified 71 accounts linked to leavers; of these, one account had been accessed after the employee's leaving date. The Integra system has a default setting that suspends access when the account is inactive for ninety days. Systems administration has closed all these accounts. There is an audit of the Integra system in the current audit plan and this area will be reviewed in more detail.

Raising debt

3.5 Services are responsible for raising their own invoices. These are recorded on the Sales Ledger (SLS) on Integra. Once raised, the value of the invoice is recorded on the ledger. The printing and posting of invoices are outsourced to an external company.

3.6 From the Integra reports for the period 9 January to 1 October 2020, analysis identified 7,794 clients with around 50,000 transactions completed. Not all accounts had been created consistently on Integra and in some instances a client has multiple accounts making risk assessment of debtors and matching of payments more difficult. There were many accounts created which did not have the postcode properly applied. **(Action a)**

Payments Process

3.7 As a result of the current COVID-19 pandemic, raising invoices for some Council services was suspended. In some circumstances, clients continued to pay for their service via a pre-arranged agreement. These payments were retained in order to prevent future hardship for the client.

3.8 A daily report is investigated for unallocated payments and these are assigned to the correct account. The most common cause of these is customers using old account reference numbers when making payment. Audit testing confirmed the completion and accuracy of these reports from day to day.

Debt management

3.9 System administration run a daily report which produces reminders, final notices, legal proceeding letters and identifies accounts requiring further action.

3.10 Audit analysis of the debtors report identified a transaction total of £4,283,134. Debts are recorded over five time periods, of this 49.6% of the transactions were over 270 days old. Income is automatically allocated to the debtors' account code however some clients are paying using old account numbers; the report records these as £203,629 unallocated credits. There is some evidence of clients having more than one account set up making it more difficult to find and allocate payments, and some spelling errors and missing information where it would be impossible to link credits to the correct account and makes tracing of debtors more difficult if required. The Debtors team has started to investigate and resolve these. **(Action b)**

3.11 In December 2019, 5,964 invoices totalling £309,742.90 were written off as per the Council's Financial Regulations. These were as a result of sequestrations, prison sentencing, insufficient information and death of the client. The overriding factor is prescribed accounts, where the client had not responded to any communications for over three years. Written off funds are reallocated to the respective Service's budget.

Reconciliations

3.12 Daily reconciliations are completed by the Debt Recovery Section. These compare sales ledger to general ledger; audit testing confirmed that these were accurately recorded.

3.13 Monthly reconciliations are completed and are independently reviewed by a manager. Audit testing confirmed that these accurately reflected the debt position.

4 Internal Audit Opinion

4.1 Overall, reasonable assurance was obtained with regard to the Accounts Receivable Service. The core function of collecting and reconciling invoice receipts is operating well. The debtors' processes were also found to be working well. However, some other issues and risks were identified during the audit which require action from the Service.

Definitions of Assurance Levels:

Substantial	The framework of governance, risk management and control is adequate and effective.
Reasonable	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
None	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

NB The level of assurance given is at the discretion of Internal Audit.

KEY FINDINGS AND ACTION PLAN
ACCOUNTS RECEIVABLE

Action	a
Finding	There are errors in creating records on the sales ledger and some information is missing or put in the wrong field.
Action Description	System users should be reminded of the correct procedure for inputting and recording information on the sales ledger.
Risk	Reconciliation and matching of unallocated credits is more difficult. It is more time consuming to trace debtors. Multiple accounts and their aggregated value may lead to debts being treated in the wrong fashion or written off as uneconomical to follow up on.
Priority (1, 2, 3)	1
Paragraph Reference	3.6
Managed by	Mark Boyd, Head of Service (Finance)
Assigned to	Moira Follan, Team Manager (Revenues)
Due Date	30 June 2021
Management Comment	An investigation has identified that the main issue relates to the inputting of postcodes in the wrong field. The Debt Recovery team has arranged for a reminder message to be included in the Integra system messages for users. This went live on 3 February 2021 and will be repeated as an annual reminder. Detailed guidance notes for users were developed during the development of the Integra system and the Debt Recovery team will arrange to email all current users to highlight the issues and re-issue the guidance notes. This will be issued by 30/04/21. The Revenues page on Connects will be reviewed and updated to provide further guidance, including links to the relevant training documents. This will be updated by 30/06/21.

Action	b
Finding	Clients have more than one account.
Action Description	Duplicate accounts should be investigated and where possible future use of these accounts should be prevented. Staff should be reminded to check existing debtors accounts before creating a new account.
Risk	Multiple accounts and their aggregated value may lead to debts being treated in the wrong fashion or written off as uneconomical to follow up on.
Priority (1, 2, 3)	1
Paragraph Reference	3.10
Managed by	Mark Boyd, Head of Service (Finance)
Assigned to	Moira Follan, Team Manager (Revenues)
Due Date	31 March 2022
Management Comment	The appropriate guidance on checking for existing accounts is detailed in the guidance notes which will be re-issued to users, as noted under Action A. Although some duplicate records are correct and have been created for business purposes, a data cleansing exercise will be undertaken during 2021/22 to identify and remove erroneous duplicates. This will be completed by 31 March 2022. As with Action A, periodic system message will be displayed reminding users of the correct procedures and encouraging them to carry out a search before adding a new customer.

Priority Key used in Action Plan

1 (High)	Control weakness where there is a material impact on the achievement of the control objectives, generally requiring prompt attention.
2 (Medium)	Control weakness which needs to be rectified, but where there is no material impact on the achievement of the control objectives.
3 (Low)	Minor weakness or points for improvement.

ACCOUNTS PAYABLE TRANSACTION TESTING Q4

1 Background

1.1 This audit used computer audit software called IDEA (Interactive Data Extraction and Analysis) to interrogate the Accounts Payable (AP) System and examined any anomalies which arose.

1.2 There were 43,575 invoices paid during the period of the audit totalling just over £151 million.

1.3 No supplier testing or advance payment testing was carried out for this audit.

1.4 The e-Procurement Officer advised that due to employees working from home, the approval process for non-PO invoices may have changed. Non-PO invoices are normally physically signed but where this is not possible, approval can be sent via email prior to keying to Integra.

2 Objectives and Scope

2.1 The main objectives of this audit were to ensure that:

- duplicate invoices have not gone undetected
- high value invoices have been properly authorised within approval limits
- invoices paid to employees are bona fide

2.2 The audit was carried out in quarter 4 and the audit period was 1st July 2020 to 31st December 2020.

3 Findings

Invoice Tests

3.1 The auditor tested for duplicate invoices for payments to suppliers and identified 102 possible duplicates that were investigated further. This confirmed that 85 were duplicates but had already been identified and action taken by the AP team. This testing therefore identified 17 potential duplicate invoices totalling £21,651.12, which have not already been identified by the AP team. The potential duplicates have been passed to the AP team to check and arrange recovery. **(Action a)**

Approval of High Value Payments

3.2 The auditor selected a sample of 20 invoices over £10,000 to check the invoices were approved by an authorised signatory, were approved within the approval limit and an independent check had been carried out. In 2/20 cases there was no 'payments over £10k' report attached so there is no evidence an independent check was carried out. In addition, 2 of the sample had a 'payments over £10k' report attached but no evidence of who had carried out the independent check. In all 4 cases the invoice was keyed by the Service.

3.3 All invoices were approved by an authorised signatory, however, in 1 case the invoice value was above their approval limit. The approver was contacted during the audit and advised they should only approve within their agreed limit and if the limit needs to be amended this needs to be agreed by their Head of Service. The Senior Payments Officer also reminded the Accounts Payable team to check the approver is an authorised signatory and amount is within their approval limit.

3.4 The net amount for payment on an interim certificate payment was zero but the £892,905 previously certified amount was paid to the supplier in error. The error was identified by the supplier, rather than our internal checks and was subsequently rectified by the AP team. It should be noted that the interim certificate should not have been passed to the AP team by the Regeneration Officer, who has an approval limit of £10k. The wrong amount was keyed by the AP team and the payments over £10k report was independently checked by the AP team.

3.5 An invoice was keyed and authorised by the HSCP Adult Finance Team using an electronic signature for the authorised for payment section of the invoice approval stamp. The auditor was advised the electronic invoice stamp with each team members electronic signature is held in the Adult Finance Team folder. Internal Audit advised the team that the electronic invoice stamp should be held on their h:drive to ensure the stamp cannot be used by anyone else to approve an invoice.

Creditors to Payroll Data Match

3.6 Testing was carried out to match employee bank details to trade and sundry supplier bank details to identify creditor payments made to employees. Excluding any matches for kinship payments there were no invoices paid to a standard supplier. There were 7 invoices paid to a sundry supplier. All were checked and there were no findings to report as all payments were bona fide payments.

4 Internal Audit Opinion

4.1 Overall, reasonable assurance was obtained with regard to the controls around the processing of invoices, in particular to preventing duplicate invoices being processed.

4.2 There is a particular concern about a single interim payment certificate for £892,905 which was paid in error and which went undetected by internal controls.

Definitions of Assurance Levels:

Substantial	The framework of governance, risk management and control is adequate and effective.
Reasonable	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
None	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

NB The level of assurance given is at the discretion of Internal Audit.

KEY FINDINGS AND ACTION PLAN
ACCOUNTS PAYABLE TRANSACTION TESTING Q4

Action	a
Finding	Testing identified 17 potential duplicate invoices totalling £21,651.12, which have not already been identified by AP.
Action Description	AP should review the potential duplicate invoices and arrange for recovery of monies paid twice.
Risk	The Council has paid the same invoice twice and the money has not been recovered.
Priority (1, 2, 3)	1
Paragraph Reference	3.1
Managed by	Mark Boyd, Head of Service (Finance)
Assigned to	Anne Lyndon, Senior Manager (Procurement)
Due Date	30.06.21
Management Comment	The Account Payable Team will investigate the 17 potential duplicates by 19th March and thereafter recover any duplicate payments.

Priority Key used in Action Plan

1 (High)	Control weakness where there is a material impact on the achievement of the control objectives, generally requiring prompt attention.
2 (Medium)	Control weakness which needs to be rectified, but where there is no material impact on the achievement of the control objectives.
3 (Low)	Minor weakness or points for improvement.

PAYROLL TRANSACTION TESTING Q3

1 Background

1.1 This audit was conducted as part of the approved 2020/21 Internal Audit Plan and used computer audit software to interrogate the HR/Payroll system and examined any anomalies which arose.

1.2 The Employee Account is used to access and complete internal online forms for contract amendments and terminations.

1.3 Mileage, travel and subsistence claims can either be submitted via the completion of a manual claim form which is then physically authorised or electronically via the system called HR21, which allows the claim form to be electronically completed and approved.

1.4 The Payroll system has a screen called Authorised Signatories which records what the employee is authorised to approve.

1.5 Audit software called IDEA (Interactive Data Extraction and Analysis) has been used to carry out this testing.

1.6 Some changes to the process had to be made due to COVID-19 with employees working from home and not being able to obtain physical signatures.

2 Objectives and Scope

2.1 The main objectives of this audit were to ensure that:

- High overtime payments are valid and properly authorised.
- Employees' last pay is correct, properly authorised and has not resulted in an overpayment.
- Salary amendments are valid and authorised.
- High mileage claims are in line with the Terms and Conditions of Employment, are valid and authorised.
- Travel and subsistence expenses are in line with the Terms and Conditions of Employment, are valid and authorised.

2.2 This testing covered the period 1st March 2020 to 30th September 2020.

3 Findings

High Overtime Payments

3.1 The auditor selected a sample of 10 high overtime payments to carry out audit testing. There were 4 overtime forms that were not approved by an authorised signatory. In 3 cases the person approving and/or their line manager has been contacted and agreed to rectify this. In the other case, the person approving overtime was temporarily covering this role.

Leavers' Last Pay

3.2 The auditor selected a sample of 10 leavers to ensure the employee's last pay is correct, the termination form has been received on a timely basis and was approved by an authorised signatory. The following was identified during the audit and rectified by Payroll:

- An employee was underpaid Pay in Lieu of Notice and Pay in Lieu of Holidays and will be paid the shortfall.
- An employee was overpaid but the overpayment amount was calculated incorrectly, and Payroll confirmed the employee will be paid the shortfall.

3.3 From the sample of 10, it was noted that 3 overpayments were made. One employee was overpaid by 3.5 months, one by 2 months and one by 2 weeks. All were picked up and rectified by Payroll.

3.4 It was noted that 7 out of 10 termination forms were received after the leaving date.

3.5 It was also noted that 3 out of 10 termination forms were not approved by an authorised signatory. One of the approvers has since been set up as an authorised signatory and the other 2 have been contacted to notify them they should not be approving termination forms unless they are an authorised signatory.

Salary Amendments

3.6 The auditor selected a sample of 10 amendment forms. It was noted that 6 of the amendment forms were not received on a timely basis as they were received after the effective date.

3.7 An amendment form had a temporary amendment end date of 11/06/21 but the Payroll system recorded this amendment had ended on 28/08/20. The auditor noted an error had been made to terminate the wrong post for this employee which resulted in the temporary amendment ending. This was rectified by the Payroll team, but the Resourcing team were not notified to allow the correct date of 11/06/21 to be recorded on the Payroll system. This was rectified by the Resourcing team during the audit.

High Mileage Claims

3.8 The auditor selected a sample of 5 high mileage claim forms. It was noted that one of the claim forms on the Expense Claim screen on the Payroll system did not show the name of the authorised signatory. Chris system admin advised there was a system error which prevented the approver information from being recorded; however, they did confirm the automatic email to the line manager was still generated so the claims were still approved even though there is no evidence of this. This has since been rectified. No other findings were noted.

Travel and Subsistence Expenses

3.9 The auditor selected a sample of 10 travel and subsistence expenses. This testing found that one of the subsistence claim forms was not submitted within 3 months and none of the 4 excess travel expenses claim forms were submitted within 4 weeks of starting at the employee's new place of employment.

3.10 The auditor contacted the 4 excess travel claimants in the audit sample to ask if they continue to travel to work or if they have been working from home since lockdown began. Two of the claimants continue to travel to work and two of the claimants have been combining working from home with travelling to work. The employees' managers have been notified of this finding. There may be other employees across the Council continuing to receive such payments since employees were sent home back in March 2020. **(action a)**

4 Internal Audit Opinion

4.1 Overall, reasonable assurance was obtained with regard to Payroll transactions testing.

Definitions of Assurance Levels:

Substantial	The framework of governance, risk management and control is adequate and effective.
Reasonable	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
None	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

NB The level of assurance given is at the discretion of Internal Audit.

KEY FINDINGS AND ACTION PLAN
PAYROLL TRANSACTION TESTING Q3

Action	a
Finding	Two of the excess travel claimants have been combining working from home with travelling to work. There may be other employees across the Council continuing to receive such payments since employees were sent home back in March 2020.
Action Description	HR/Payroll should remind services to review the excess mileage payments where staff have changed work location.
Risk	Overpayments have gone undetected if claimants have been working from home during lockdown.
Priority (1, 2, 3)	2
Paragraph Reference	3.10
Managed by	Fiona Walker, Head of Service (People and ICT)
Assigned to	Jackie Hamilton, Senior Manager Employee Services
Due Date	Complete
Management Comment	A report has been extracted of all employees who are receiving payment in respect of excess travel, this has been compared to records held in relation to the COVID impact on the workforce (home working). This extract has been sent to Heads of Service, who have been requested to review the records for accuracy and instruct Payroll where the payment should cease or be amended.

Priority Key used in Action Plan

1 (High)	Control weakness where there is a material impact on the achievement of the control objectives, generally requiring prompt attention.
2 (Medium)	Control weakness which needs to be rectified, but where there is no material impact on the achievement of the control objectives.
3 (Low)	Minor weakness or points for improvement.

ALLOWANCES AND PAY ADJUSTMENTS

1 Background

1.1 This audit reviewed the processes surrounding the payment of allowances and pay adjustments.

2 Objectives and Scope

2.1 The key objectives of this audit were to ensure that: -

- allowance payments are being appropriately authorised,
- regular reviews of those receiving allowances are being undertaken
- evidence of the reason for, and calculation of, pay adjustments is being retained

3 Findings

AUTHORISATION OF ALLOWANCES

3.1 The Council's 'Terms and Conditions of Employment' set out a number of allowances which employees may be entitled to.

3.2 Responsibility for confirming entitlement lies with the council officer who instructs Employee Services to pay the allowance.

3.3 A sample of payments were selected for testing from the following allowance categories: -

- Mental Health Officer Allowance
- Unsocial Hours Allowance
- Responsibility Allowance

3.4 Audit testing identified allowances being approved by council officers who are not authorised signatories. Employee Services sample check 10% of authorisations, but in general, reliance is placed on the individual officer signing the form to be aware of their own authority levels. **(action point a)**

REVIEW OF ALLOWANCES

3.5 Employee Services carry out an annual employee data check. Services are provided with employee details and asked to check that the salaries, allowances and hours listed are accurate. This check wasn't undertaken in 2020 due to Coronavirus creating huge demands on staff time, however Employee Services have confirmed that the task is on their work schedule to be carried out in 2021.

3.6 A detailed check on the unsocial hours' allowances being paid is also carried out annually. Services are required to confirm the rate to be paid to each employee.

3.7 It was found that the spreadsheets were being authorised by an image of the authorised signatory's signature being copied and pasted into the spreadsheet. This could be completed by someone other than the authorised signatory and is not deemed as enough evidence of authorisation for audit purposes. Going forward, Employee Services have agreed that authorisation of these completed spreadsheets will be evidenced by the e-mail from the authorised signatory returning the spreadsheet.

PAY ADJUSTMENTS

3.8 Pay adjustments are required when a one-off adjustment to an employee's salary is necessary - for example to correct a prior error or to make a backdated payment.

3.9 Employee Services calculate the pay adjustment.

3.10 Whilst Employee Services keep copies of correspondence resulting in a pay adjustment (such as emails, contract amendment forms), they do not retain a copy of the manual calculation undertaken to work out the value of the pay adjustment.

3.11 Should a query be received regarding a pay adjustment, Employee Services would have to re-create the original calculation.

3.12 In order to confirm that sufficient information is being retained to allow this recalculation to happen if required, Audit requested that Employee Services provide detailed workings for a sample of 5 pay adjustments.

3.13 Employee Services were able to provide detailed calculations for each item in the sample and whilst 1 error was identified, this was due to human error as opposed to an issue with the process. Employee Services corrected the error immediately.

3.14 Audit noted that 4 out of the 5 pay adjustments tested were necessary because of delayed submission of forms by Services. **(action point b)**

4 Internal Audit Opinion

4.1 Overall, substantial assurance was obtained with regard to the processes surrounding the payment of allowances and pay adjustments.

4.2 Audit testing highlighted that Services play a critical role in ensuring the accuracy of allowance payments and minimising the need for pay adjustments. Errors or delays in submitted forms by Services directly impacts upon the workload of Employee Services and the take home salary of employees.

Definitions of Assurance Levels:

Substantial	The framework of governance, risk management and control is adequate and effective.
Reasonable	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
None	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

NB The level of assurance given is at the discretion of Internal Audit.

KEY FINDINGS AND ACTION PLAN
ALLOWANCES AND PAY ADJUSTMENTS

Action	a
Finding	Allowance forms are being signed by Officers who do not have the authority to do so.
Action Description	Employee Services to remind Managers that they must ensure they have authorised signatory status before signing any payroll forms.
Risk	Fraudulent or erroneous allowance payments being made to employees
Priority (1, 2, 3)	1
Paragraph Reference	3.4
Managed by	Fiona Walker (Head of Service, People & ICT)
Assigned to	Jackie Hamilton (Senior Manager, Employee Services)
Due Date	Complete
Management Comment	An email has been issued to Heads of Service with a copy also posted on the Senior Managers Network Teams site. The email outlines the payroll transactions that require to be approved by an authorised signatory, how to request information on who their signatories are and also the document to add any new signatories.

Action	b
Finding	Delays in the submission of forms to Employee Services are resulted in pay adjustments being necessary.
Action Description	Employee Services to remind Managers that they must submit forms timeously to prevent incorrect payment of employees.
Risk	Employees are not receiving the correct remuneration for the employment
Priority (1, 2, 3)	3
Paragraph Reference	3.14
Managed by	Fiona Walker (Head of Service, People & ICT)
Assigned to	Jackie Hamilton (Senior Manager, Employee Services)
Due Date	Complete
Management Comment	An email including a link to payroll deadlines has been issued to all authorised signatories to remind them of the requirement to submit accurate and timely information to the Payroll Team.

Priority Key used in Action Plan

1 (High)	Control weakness where there is a material impact on the achievement of the control objectives, generally requiring prompt attention.
2 (Medium)	Control weakness which needs to be rectified, but where there is no material impact on the achievement of the control objectives.
3 (Low)	Minor weakness or points for improvement.

HRA PLANNED MAINTENANCE AND REACTIVE REPAIRS

1 Background

1.1 This area was last audited in 2015/16. Only revenue spend has been reviewed during the audit.

2 Objectives and Scope

2.1 The objectives of this audit were to ensure that:-

- There is a process for monitoring planned maintenance to ensure works are being completed timeously
- Emergency and right to repair repairs are being carried out in line with prescribed timescales
- Standing Orders relating to Contracts have been adhered to when appointing external contractors

3 Findings

Planned Maintenance

3.1 The process for carrying out annual gas safety checks was reviewed.

3.2 The Council's contractor takes the lead in this process.

3.3 The contractor is responsible for arranging access to properties and updating the Council's records on all completed checks daily.

3.4 Audit obtained a list of all properties due a gas safety check in order to assess how many are overdue. Out of 12,060 properties (this includes all properties requiring a gas safety check, not just HRA properties) only 345 checks were overdue as at 1 April 2021. This represents less than 3% of the total properties.

3.5 The Council and the contractor are actively working to gain access to carry out these outstanding checks, via forced entry if necessary.

Emergency and Right to Repair Repairs

3.6 When repairs are reported to the Council they are classed as either:-

- Emergency
- Right to Repair
- Non-emergency

3.7 The classification defines the timescale for completing the repair.

3.8 Tenants are made aware of the above via the Council's Housing Repairs Policy.

3.9 Emergency repairs should be completed within 4 hours.

3.10 In order to ensure emergency repairs are being completed timeously, a report of all jobs classified as emergency in 2020/21 was obtained from Building Services.

3.11 The report gives a due date and time for each repair along with a completion date and time. Audit compared these and found that more than 94% of all repairs were completed within the 4-hour deadline.

3.12 Further investigation showed that the majority of the 'late jobs' were completed within a further 2 hours of the original deadline (i.e. within 6 hours), with only 1.4% taking longer than this.

3.13 The Housing (Scotland) Act 2001 sets out certain repairs that must be done within a predefined timescale. Depending on the works, the timescale for completion can be either 1,3 or 7 days.

3.14 If the Council fails to complete the repair within the timescale, tenants are entitled to claim compensation.

3.15 In order to ensure Right to Repair repairs are being completed timeously, a report of all jobs classified as Right to Repair in 2020/21 was obtained from Building Services.

3.16 The report gives a due date for each repair along with a completion date. Audit compared these and found that all repairs had been completed within the relevant timescale.

External Contractors

3.17 Audit testing focussed on non-emergency repairs carried out by external contractors in order to confirm that the Council's procurement procedures are being adhered to.

3.18 For a sample of payments, the auditor ensured that:-

- the contractor was listed on the Council's contract register
- the invoice had been authorised by an authorised signatory

3.19 All contractors tested were found to be approved suppliers per the contract register.

3.20 One instance of an invoice being approved by a council officer without the appropriate authority was noted during Audit testing. This was not picked up by Accounts Payable prior to keying the invoice.

3.21 The Service has spoken to the member of staff and confirmed the individual now has a clear understanding of personal authority levels going forward. In addition, Accounts Payable have recently implemented a new, more robust, process for checking authority levels prior to keying invoices which should further prevent such an instance going forward.

4 Internal Audit Opinion

4.1 Overall, substantial assurance was obtained with regard to the processes for dealing with planned, emergency and non-emergency repairs.

Definitions of Assurance Levels:

Substantial	The framework of governance, risk management and control is adequate and effective.
Reasonable	Some improvements are required to enhance the adequacy and effectiveness of the framework of governance, risk management and control.
Limited	There are significant weaknesses in the framework of governance, risk management and control such that it could be or could become inadequate and ineffective.
None	There are fundamental weaknesses in the framework of governance, risk management and control such that it is inadequate and ineffective or is likely to fail.

NB The level of assurance given is at the discretion of Internal Audit.