NORTH AYRSHIRE COUNCIL

30 May 2024

Audit and Scrutiny Committee

Title:	**Internal Audit Reports issued**
Purpose:	To inform the Committee of the findings of Internal Audit work completed between March and April 2024.
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 between March and April 2024. 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 three 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
Procurement Cards	Substantial
Cyber Resilience Business Continuity	Reasonable/Limited
Ayrshire Growth Deal – Revenue Projects	Substantial

3. Proposals

3.1 It is proposed that the Committee considers the outcomes from the Internal Audit work completed between March and April 2024.

4. Implications/Socio-economic Duty

Financial

4.1 None.

Human Resources

4.2 None.

Legal

4.3 None.

Equality/Socio-economic

4.4 None.

Climate Change and Carbon

4.5 None.

Key Priorities

4.6 The work of Internal Audit helps to support the efficient delivery of the strategic priorities within Our Council Plan 2023-2028.

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 **Laura Miller, Senior Manager (Audit, Fraud, Safety and Risk),** on **01294 324524**.

Background Papers
None.

PROCUREMENT CARDS

1 Background

1.1 When procurement cards are used in line with Council guidance they provide a number of benefits to both Services and the Council as a whole. These include:-

- significant time savings from processing less purchase orders and invoices
- one payment per month per card, from the council to the bank eliminating multiple payments
- reduction in petty cash purchases and cash holdings
- opportunity to purchase items at lower cost through internet
- clear audit trails.

2 Objectives and Scope

2.1 The objective of this audit was to ensure:-

- The number of cards in issue is being controlled and reviewed
- Access to imprest (cash) is controlled, and not automatically granted to all cardholders
- Transactions are being reviewed and approved timeously.

3 Findings

3.1 In 2023 all Services were instructed to review and, if necessary, rationalise the number of procurement cards allocated to their officers.

3.2 eProcurement also carried out a review of the data within SDOL in 2023.

Cardholders

3.3 All applications for a procurement card must be made via an eform. Within the eform:-

- Applicants must confirm they have completed online procurement card training
- Applicants must confirm if the imprest function requires to be activated on the card
- Applicants must detail the type of purchases they intend to make with the card and (if applicable) imprest
- Applications must be approved by an officer of Grade 14 or above, with the exception of HSCP officers who have their applications approved by the Head of Service (HSCP Finance & Transformation).

3.4 The above controls ensure that only those with a genuine business need are approved for a procurement card.

3.5 A comparison of the number of cardholders between February 2024 and March 2023 confirmed an overall reduction in the number of procurement cards from 360 to 295. All Services have either maintained or reduced the number of cards allocated to their officers. The following table summarises the comparison results:-

Directorate	Service	No of cardholders Feb 24	No of cardholders Mar 23	Movement - increase/(reduction)
Chief Executive	Democratic Services	8	8	0
Chief Executive	Financial Services	4	6	-2
Chief Executive	People & ICT	12	22	-10
Communities & Education	Connected Communities	11	15	-4
Communities & Education	Education	126	146	-20
HSCP	Chief SW Officer	0	4	-4
HSCP	Child, Families&Justice	17	23	-6
HSCP	Financial Inclusion	0	2	-2
HSCP	Health & Community Care	8	9	-1
HSCP	HSCP Business Admin	52	58	-6
HSCP	HSCP Finance & Transform	5	7	-2
HSCP	Mental Health	1	2	-1
Place	Directorate Supp - Place	4	4	0
Place	Economic Dev,Growth&Reg	5	5	0
Place	Housing & Public Protect	26	30	-4
Place	Neighbourhood Services	11	14	-3
Place	Sus, TPT & Corp Property	5	5	0
		295	360	-65

Imprest

3.6 Activating the imprest function allows a cardholder to withdraw cash using their procurement card.

3.7 Cardholders are not automatically granted access to this function – it must be requested, justified and approved. For new cardholders this is done as part of the application process (as detailed in **3.3** above). For existing cardholders, the request is made via email.

3.8 Audit reviewed the number of cards with the imprest function activated in February 2024 as compared to March 2023.

3.9 The number of cards with the imprest function activated has increased over the review period from 91 in March 2023 to 119 in February 2024.

3.10 Audit discussed this increase with eProcurement. eProcurement explained that the number of imprest users reported as at March 2023 is artificially low. Whilst preparing user reports for Services to review, an issue with the recording of cardholder function access was identified. Reports were not flagging a number of imprest users as having the function when they did, in fact, have it.

3.11 eProcurement immediately reviewed all cardholders records and updated as necessary. This update resulted in a revised figure of 130 imprest users. Reports were not circulated to Services until this exercise was complete.

3.12 Audit selected a sample of 10 users who have been given imprest status in SDOL between March 2023 and February 2024 for detailed review.

3.13 5 of the 10 were genuine new imprest users. Audit reviewed the application process for each of these users. All stages of the process as set out in **3.7** have been completed and documented.

3.14 The remaining 5 were not genuine new users but were picked up as such by Audit testing due to the error noted in **3.11.** For each of these users, Audit ensured the report provided to Services for review was reflecting the true access status of the user. No issues were noted during testing.

Monitoring

3.15 Card transactions are not posted to Integra until they have been both reviewed (by the cardholder) and approved (by the approver) in SDOL. Delays in this approval process can impact on budget monitoring.

3.16 Every month emails are sent to all reviewers and approvers reminding them of the need to review or approve any outstanding transactions.

3.17 In addition, eProcurement produce a quarterly report of outstanding transactions for circulation to senior managers. Managers are responsible for reviewing this report and taking action to address any issues highlighted.

3.18 Audit obtained details of all outstanding transactions as at 4 January 2024 and calculated the age of the transaction per Directorate. The following table summarises these results:-

Days outstanding	Number of oustanding transactions	Value of outstanding transaction
0-50	1,547	338,172.92
51-100	212	19,270.04
101-200	113	10,096.29
201-300	81	7,400.00
301-400	16	1,040.62
401-500	12	2,100.72
501-600	7	429.86
601-700	8	632.47
Grand Total	1,996	379,142.92

3.19 Based on the above, most transactions are being both reviewed and approved within the first 50 days.

3.20 The number of transactions outstanding for more than 50 days has reduced over the review period – in January 2024 there were 449 outstanding as compared to 767 in March 2023.

3.21 Imprest withdrawals remain outstanding on SDOL until the cash has been spent in full. This will account for some of the transactions outstanding for more than 50 days, and is not necessarily reflective of poor transaction management.

4 Internal Audit Opinion

4.1 Overall, substantial assurance was obtained with regard the controls surrounding the issuing and ongoing monitoring of procurement cards.

Definitions of Assurance Levels:

Substantial	A sound system of governance, risk management and control exist, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
None	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

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

CYBER RESILIENCE BUSINESS CONTINUITY

1 Background

1.1 Business continuity was last audited in 2018/19.

1.2 The audit program is based on Section 14 of the Public Sector Cyber Resilience Framework which is called Business Continuity. The overall objective is to ensure information security continuity shall be embedded in the organisation's business continuity management systems.

Section 14 covers the following 6 areas, all of which will be included in the audit:

- data recovery capability,
- backup policies and procedures,
- disaster recovery policies and procedures,
- business continuity & disaster recovery testing policies and procedures,
- Data Protection Impact Assessments and
- business continuity contingency plans.

1.3 IT Services are responsible for the backup process within the Council's data centres. Audit testing has been restricted to the IT backup process.

1.4 A sample of business continuity plans that reference key IT systems were selected for audit testing. The same key IT systems were used to test Data Protection Impact Assessment.

2 Objectives and Scope

2.1 The objectives of the audit were to ensure that:

- Recovery controls are in place to protect against information/data being lost or compromised.
- Backup copies of information, software and system images shall be taken and tested regularly.
- The Council has well defined and tested processes in place to ensure the continuity of key operational services in the event of failure or compromise.
- Scenario-based exercises and processes to test recovery response plans are planned and performed.
- DPIAs are undertaken to determine the impact of the intended processing on the protection of personal data where the processing is likely to result in a high risk to the rights and freedoms of individuals. The DPIA should consider the technical and organisational measures necessary to mitigate that risk.
- Contingency mechanisms are in place to continue to deliver services in the event of any failure or compromise of any system or service.

3 Findings

Data Recovery Capability

3.1 Site Recovery Manager (SRM) is the disaster recovery product used for Windows servers and IT provided a list of what is managed via this process. This allows a

quicker recovery of all servers on the list instead of restoring each server individually. There is a separate disaster recovery process in place for Unix servers which also allows for a quicker recovery of such servers instead of restoring each server individually. The Council's key IT systems have data recovery capability. There are a number of locally stored IT systems not covered by the SRM or Unix disaster recovery process and there is no priority list to decide which order these IT systems are recovered in the event of a major cyber security event. **(action a)**

3.2 The auditor reviewed the Site Recovery Manager list of servers and compared this to the Commvault backup schedule report. This test identified a server on Site Recovery Manager that cannot be matched to a backup plan on the Commvault backup schedules report. IT has provided evidence this has now been allocated to a backup plan.

Backup Policies and Procedures

3.3 Commvault Hyperscale is the backup product for on-premise infrastructure and IT systems. Data stored in the primary data centre is backed up to a secondary data centre which is at a different physical location and a third copy is stored offsite using a cloud product. The secondary data centre also provides a second site for data recovery capability in the event of a disaster but there is limited capability at the second site.

3.4 The auditor reviewed the Commvault schedules report which lists all servers, their associated backup plan and evidence of when the last backup was taken. The auditor checked the backup process at a point in time and confirmed the backups were successful. However, it should be noted there were a number of servers that were not allocated to a backup plan. IT Services advised there is some housekeeping required to clean up the Commvault schedule, most of which are due to old servers that no longer need to be allocated to a backup plan but can still be used to restore historical backups. IT reviewed and cleaned the Commvault schedule during the course of the audit and also advised that going forward, ITSM requests should be made to decommission servers and this includes a task to remove it from the backup plan.

3.5 Commvault Metallic is the product which is used to provide additional offsite backup for the M365 application data. This includes the back up of data for Exchange, SharePoint, OneDrive and Teams. This backup is taken every 8 hours and there is a Metallic Commvault console which is used to monitor and control this backup process. The auditor checked the status of this backup process at a point in time and there were no findings to report.

Disaster Recovery Policies and Procedures

3.6 IT Services provided a copy of the Disaster Recovery (DR) plans overview spreadsheet which lists 91 DR plans across the different areas within IT and it also lists 650 historical DR plans. Initially, there was information missing but IT have since updated this to ensure the last review date for completed plans and expected completion dates for incomplete plans are now recorded. There are 51 plans with the status 'complete' or 'awaiting review', 38 plans have the status 'under development' or 'not started' and 2 plans have no status recorded. The

Team Manager (Operations) advised the historical data will be deleted, this spreadsheet will be moved to a SharePoint list and have a flow that will automatically email plan owners at 12 months to review or remove if the solution has been decommissioned. In addition, monthly DR meetings are now scheduled to progress the completion of outstanding DR plans. **(action b)**

3.7 The DR plans reviewed by the auditor do not document the recovery time objective (RTO) for the operational service. The Team Manager (Operations) advised this is difficult to calculate given the different scenarios that could impact it but agreed an average RTO should be added to the DR plans. **(action c)**

BC/DR Testing Policies and Procedures

3.8 IT Services have identified the need to test the backup and disaster recovery processes on a quarterly basis. Testing is planned to start in quarter 1 of 2024/25 for Windows Server test restore, Site Recovery Manager test recovery, Database test restore, Unix server test restore and network device test restore. Testing for M365 test restore began in Q3 2023/24. In addition, the planned Business Continuity and Disaster Recovery Test Plan exercises have been rescheduled to start again in 2024/25. They have been delayed due to a vacant Team Manager (ICT and Cyber Security) post that has now been filled. **(action d)**

Data Protection Impact Assessments (DPIA)

3.9 There is a Data Protection Impact Assessment SharePoint page on Connects which provides information on this process and provides a link to the Data Protection Impact Assessment Information and Guidance document; however, this document was last reviewed and updated on 20th December 2018. Information Governance advised this has been identified as needing to be reviewed and updated. **(action e)**

3.10 Information Governance have recently introduced a DPIA tracker to allow all DPIA's to be recorded and monitored. This documents what stage they are at so the team can be more proactive at chasing up outstanding actions and ensuring annual reviews are carried out. A review of the DPIA tracker identified a significant backlog of completed DPIA's awaiting sign off by the Data Protection Officer. There were 56 completed DPIA's waiting on being signed off at the time of the audit. There have been resourcing issues in the team which have since been resolved. **(action f)**

3.11 A DPIA has not been completed for the CM2000 system. This should be completed retrospectively and passed to the Data Protection Officer to sign it off. **(action g)**

3.12 A DPIA had not been completed for the CareFirst system. Given that the implementation of the replacement system (Eclipse) is not imminent, Information Governance confirmed a DPIA for the CareFirst system should still be completed. A DPIA was completed during the course of the audit. An older template has been used and it has not yet been passed to the Data Protection Officer to sign it off. **(action h)**

3.13 A DPIA has not been completed for the Civica system used by Housing Services (this system was previously called Abritas). This should be completed retrospectively and passed to the Data Protection officer to sign off. **(action i)**

3.14 A DPIA was completed for the Flexiroute system; however, this was completed in an old format and was not signed off by the Data Protection Officer. Information Governance advised the DPIA should be reviewed, transferred to the new template and passed to the Data Protection Officer to sign it off. **(action j)**

BC Contingency Plan

3.15 The Council has a Business Continuity Management (BCM) Strategy in place, however, this strategy was last updated in October 2015. The Team Manager (Risk) is aware of this and the document is currently being updated. **(action k)**

3.16 The Business Continuity Plan Template includes the threat scenario for the loss of ICT. The template does not advise requesting a copy of the cloud provider's BC plan where the lead officer/plan owner has identified a cloud hosted system is being used.
(action l)

3.17 Internal Audit reviewed the Care at Home Business Continuity Plan to ensure the CM2000 system is properly documented within this plan. The plan was last updated on 18/12/23 but this version should be saved in the Business Continuity Management Hub. The Senior Manager (Locality Services) advised the provider has been contacted more than once to request a copy of their business Continuity plan as this is a cloud based system. Once received, the Senior Manager (Locality Services) has been advised to reference this document in the Care at Home Business Continuity Plan.

3.18 Internal Audit reviewed the Corporate Transport Hub Business Continuity Plan to ensure the Flexiroute system is properly documented within this plan. The plan has not been updated since 15/11/21 and one of the response team members left in August 2023. The Flexiroute system is not listed as one of the ICT systems/applications under the Loss of IT section which means the details of arrangements the service has in place if this system is not available has not been recorded and the back-up storage information for this system has not been recorded. This is a cloud hosted system, but a copy of the cloud providers BC plan has not been obtained and referenced in this BC plan. **(action m)**

4 Internal Audit Opinion

4.1 Limited assurance was obtained with regards to the DPIA section of the audit due to all 4 IT systems selected in the audit sample either having no DPIA in place or no completed DPIA signed off by the DPO. In addition, there is a significant backlog of DPIA's awaiting sign off by the Data Protection Officer to ensure the DPIA's have been reviewed and any necessary DPO advice provided.

4.2 Reasonable assurance was obtained with regards to the other 5 sections of the audit. The recommendations made will assist the Council to strengthen the response to a cyber security event, particularly in relation to a priority recovery list for IT systems not covered by the SRM or Unix recovery process, outstanding DR

plans being completed so they can be followed when needed, and rigorous testing of the BC/DR process and the restore and recovery process.

Definitions of Assurance Levels:

Substantial	A sound system of governance, risk management and control exist, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
None	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

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

KEY FINDINGS AND ACTION PLAN
CYBER RESILIENCE BUSINESS CONTINUITY

Action	a
Finding	The Council's key IT systems have data recovery capability. There are a number of locally stored IT systems not covered by the SRM or Unix disaster recovery process and there is no priority list to decide which order these IT systems are recovered in the event of a major cyber security event.
Action Description	IT Services in consultation with the Risk Manager should compile an IT Corporate Systems list and facilitate a discussion with ELT to enable a Corporate priority list for the recovery of locally stored IT systems not covered by the SRM or Unix disaster recovery process.
Risk	No clear prioritised order for recovery could result in a delay in the recovery of such systems.
Priority (1, 2, 3)	2
Paragraph Reference	3.1
Managed by	Fiona Walker, Head of Service (People & ICT)
Assigned to	James McNeil, Senior Manager (ICT)
Due Date	31st October 2024
Management Comment	All council systems are backed up by our Backup and Recover solution, CommVault. However, Site Recovery Manager can be used to quickly recover systems in the event of a disaster scenario to our DR site. This is limited to 40 systems. IT will consult with the Risk Manager to compile a list of systems that could be sorted into a prioritised list for recovery. Once agreed, IT would then put the highest priority systems on SRM and have a priority list for servers out with SRM, "local", to be restored in order that is beneficial to the business. UNIX based applications are automatically covered by the UNIX DR process.

Action	b
Finding	There are 51 DR plans with the status 'complete' or 'awaiting review', 38 plans have the status 'under development' or 'not started' and 2 plans have no status recorded. The Team Manager (Operations) advised the historical data will be deleted, this spreadsheet will be moved to a SharePoint list and have a flow that will automatically email plan owners at 12 months to review or remove if the solution has been decommissioned. In addition, monthly DR meetings are now scheduled to progress the completion of outstanding DR plans.
Action Description	IT Services should continue to progress the completion of outstanding DR plans, ensure all DR plans have been reviewed at least annually and delete historical DR data no longer required.
Risk	Having no DR plan or an out of date or inaccurate data in the DR plan could result in a delay in the recovery process.
Priority (1, 2, 3)	2
Paragraph Reference	3.6

Managed by	Fiona Walker, Head of Service (People & ICT)
Assigned to	James McNeil, Senior Manager (ICT)
Due Date	Complete
Management Comment	SharePoint Document Library has now been created for current and future DR plans. Document Library is set to trigger an email to the plan owner when the last review date hits 12 months to ensure the plans are reviewed again. Legacy plans have been removed. IT continually work to review and develop DR plans for systems.

Action	c
Finding	The DR plans reviewed by the auditor do not document the recovery time objective (RTO) for the operational service. The Team Manager (Operations) advised this is difficult to calculate given the different scenarios that could impact it but agreed an average RTO should be added to the DR plans.
Action Description	Realistic RTOs should be agreed and recorded in the DR plans.
Risk	If RTO's are not known, services are not sure how long it will take to recover the system or service and cannot plan accordingly.
Priority (1, 2, 3)	2
Paragraph Reference	3.7
Managed by	Fiona Walker, Head of Service (People & ICT)
Assigned to	James McNeil, Senior Manager (ICT)
Due Date	Complete
Management Comment	Recovery Time objectives have now been added to current DR plans and will be incorporated in all future plans that are created. RTO (Single Server failure): Two Working Days RTO (Full Failure | SRM/UNIX Replication): Five Working Days RTO (Full Failure | Backup Only): 8 to 12 Weeks

Action	d
Finding	IT Services have identified the need to test the backup and disaster recovery processes on a quarterly basis. Testing is planned to start in quarter 1 of 2024/25 for Windows Server test restore, Site Recovery Manager test recovery, Database test restore, Unix server test restore and network device test restore. Testing for M365 test restore began in Q3 2023/24. In addition, the planned Business Continuity and Disaster Recovery Test Plan exercises have been rescheduled to start again in 2024/25. They have been delayed due to a vacant Team Manager (ICT and Cyber Security) post that has now been filled.
Action Description	IT Services should start completing the planned backup and disaster recovery testing and ensure this testing is completed at least quarterly. The planned Business Continuity and Disaster Recovery exercises should be recommenced as soon as possible.

Risk	Issues identified at testing are not identified prior to a live scenario; the necessary data is not available for recovery; the backup cannot be relied upon to restore as expected.
Priority (1, 2, 3)	2
Paragraph Reference	3.8
Managed by	Fiona Walker, Head of Service (People & ICT)
Assigned to	Gavin Alston, Team Manager (ICT & Cyber Security)
Due Date	30th June 2024
Management Comment	IT have a Backup & Recovery testing schedule and tests have been scheduled on a quarterly basis from April 2024.

Action	e
Finding	There is a Data Protection Impact Assessment SharePoint page on Connects which provides information on this process and provides a link to the Data Protection Impact Assessment Information and Guidance document; however, this document was last reviewed and updated on 20th December 2018. Information Governance advised this has been identified as needing to be reviewed and updated.
Action Description	The Data Protection Impact Assessment Information and Guidance document should be reviewed, updated and reissued to ensure staff are aware of the need to complete DPIA's.
Risk	It is not in line with industry best practice; out of date or inaccurate information.
Priority (1, 2, 3)	2
Paragraph Reference	3.9
Managed by	Aileen Craig, Head of Service (Democratic)
Assigned to	Lauren Lewis, Data Protection Officer
Due Date	Completed
Management Comment	This action was in hand at the time of the audit. The action has been completed and the 2024 version has been uploaded to Connects. Mandatory Information Management training which is to be undertaken by all staff on an annual basis highlighting requirements, including criteria on when DPIAs are required is in place.

Action	f
Finding	A review of the DPIA tracker identified a significant backlog of completed DPIA's awaiting sign off by the Data Protection Officer. There were 56 completed DPIA's waiting on being signed off at the time of the audit.
Action Description	The Information Governance team should prioritise clearing the backlog to ensure completed DPIA's are signed off as soon as possible.
Risk	Potential non-compliance with Data Protection Legislation; Council reputational damage; Council could be subject to enforcement action by the Information Commissioner's Office;

	Delays to improvement projects while awaiting sign off of the DPIA.
Priority (1, 2, 3)	1
Paragraph Reference	3.10
Managed by	Aileen Craig, Head of Service (Democratic)
Assigned to	Lauren Lewis, Data Protection Officer
Due Date	Completed
Management Comment	The number of DPIAs received by the Information Governance Team varies as business is put to the Team for consideration and review. A number of these involve consideration of complex and emerging issues which require detailed investigation. The Information Governance team has now been augmented to ensure that there are more staff members in post to deal with DPIAs. The tracker has been reviewed and updated to reflect the various stages of DPIAs with the current levels of outstanding DPIAs for Information Governance Team review being 18 (17 for DPO sign off and 1 for review). At the time of completion, 39 DPIAs have been returned to Services for further feedback and updating with relevant information. An online form is now live to log DPIA requests via EMPro. This further facilitates both reporting functionality and annual review processes for the Information Governance Team; coupled with additional resource this will enhance service performance and compliance in this area.

Action	g
Finding	There is no DPIA for the CM2000 system.
Action Description	A DPIA should be completed retrospectively for the CM2000 system and this should be passed to the Data Protection Officer to sign off.
Risk	Non-compliance with Data Protection Legislation; Personal data is at risk of misuse; Council reputation damage; Council could be subject to enforcement action by the Information Commissioner's Office.
Priority (1, 2, 3)	1
Paragraph Reference	3.11
Managed by	Kerry Logan, Head of Service (Health & Community Care)
Assigned to	Lorraine Dyet (Senior Manager)
Due Date	30 April 2024
Management Comment	The CM2000 Monitoring Officer within the HSCP is currently progressing the completion of a DPIA, and is engaging with the Data Protection Officer with the aim of completing this by the end of April 2024.

Action	h
Finding	A DPIA had not been completed for the CareFirst system. A DPIA was completed during the course of the audit. An older template has been used and it has not yet been passed to the Data Protection Officer to sign it off.
Action Description	The DPIA should be transferred to the new template and passed to the Data Protection Officer to sign off.

Risk	Non-compliance with Data Protection Legislation; Personal data is at risk of misuse; Council reputation damage; Council could be subject to enforcement action by the Information Commissioner's Office.
Priority (1, 2, 3)	1
Paragraph Reference	3.12
Managed by	Paul Doak, Head of Service (HSCP Finance & Transformation)
Assigned to	Neil McLaughlin, Team Manager (Information Systems)
Due Date	Complete
Management Comment	The CareFirst system was introduced in North Ayrshire in 2001. The DPIA which was prepared during the course of the audit has now been updated onto the new template and signed off by the Data Protection Officer.

Action	i
Finding	There is no DPIA for the Civica system used by Housing Services.
Action Description	A DPIA should be completed retrospectively for the Civica system used by Housing Services and this should be passed to the Data Protection Officer to sign off.
Risk	Non-compliance with Data Protection Legislation; Personal data is at risk of misuse; Council reputation damage; Council could be subject to enforcement action by the Information Commissioner's Office.
Priority (1, 2, 3)	1
Paragraph Reference	3.13
Managed by	Yvonne Baulk, Head of Service (Housing & Public Protection)
Assigned to	Fiona Ellis, Senior Manager (Housing Strategy & Development)
Due Date	31/05/24
Management Comment	The Digital team are actively working to pull together the DPIA for the Civica system to coincide with a major system upgrade and Trust Housing coming on board with the North Ayrshire Housing Register (NAHR). The team are liaising with the Information Governance team in preparing the draft DPIA which requires to be approved by them in the first instance. Input from the Registered and Social Landlords that utilise the NAHR is also required and is ongoing at present.

Action	j
Finding	A DPIA was completed for the Flexiroute system; however, this was completed in an old format and was not signed off by the Data Protection Officer.
Action Description	The DPIA for the Flexiroute system should be reviewed, transferred to the new template and passed to the Data Protection Officer to sign it off.
Risk	Non-compliance with Data Protection Legislation; Personal data is at risk of misuse; Council reputation damage; Council

	could be subject to enforcement action by the Information Commissioner's Office.
Priority (1, 2, 3)	1
Paragraph Reference	3.14
Managed by	Gordon Mitchell, Senior Manager (Transport)
Assigned to	Susan Adamson, Team Manager (Journeys & Hires /Transport)
Due Date	31/05/2024
Management Comment	The original DPIA was transferred onto the appropriate new format and passed to the Data Protection Officer to review and signoff. However, this has since been returned with comments and further recommendations. Due to the nature and sensitivity of the Personal Information held, shared, and processed, it was a recommendation of the DPO that the completion of the DPIA should be supported with a collaborative approach of Senior Managers from both the Health & Social Care Partnership and Education and Youth Employment as the key information providers. A meeting has been arranged with representation from both services and the Information Governance team with a view of a satisfactory sign off by the end of May 2024.

Action	k
Finding	The Council has a Business Continuity Management (BCM) Strategy in place, however, this strategy was last updated in October 2015. The Team Manager (Risk) is aware of this, and the document is currently being updated.
Action Description	Once the updated Business Continuity Management Strategy has been agreed it should be reissued to ensure relevant staff are aware the strategy has been reviewed and updated.
Risk	It is not in line with industry best practice; out of date or inaccurate information.
Priority (1, 2, 3)	2
Paragraph Reference	3.15
Managed by	Mark Boyd, Head of Service (Finance)
Assigned to	Alex Fitzharris, Team Manager (Risk & Insurance)
Due Date	29 November 2024
Management Comment	The BCM strategy has been revised and reviewed and is currently subject to further review and amendments ahead of formal approval process.

Action	l
Finding	The Business Continuity Plan Template includes the threat scenario for the loss of ICT. The template does not advise requesting a copy of the cloud provider's BC plan where the lead officer/plan owner has identified a cloud hosted system is being used.
Action Description	The Business Continuity Plan Template should be amended to advise that where a cloud hosted system has been identified, a copy of the cloud provider's BC plan should be obtained and referenced in the BC plan.

Risk	Cloud providers resiliency is not known; delay in recovering from an incident.
Priority (1, 2, 3)	2
Paragraph Reference	3.16
Managed by	Mark Boyd, Head of Service (Finance)
Assigned to	Alex Fitzharris, Team Manager (Risk & Insurance)
Due Date	29 November 2024
Management Comment	A working group will be set up with officers from across the Council to revise the BC Plan Template approach considering the release of the Business Continuity Institutes Good Practice Guidelines 7.0 (2023). The BC plan template changes will be incorporated into the wider BCM Strategy review work.

Action	m
Finding	The Corporate Transport Hub Business Continuity has not been updated since 15/11/21 and one of the response team members left in August 2023. The Flexiroute system is not listed as one of the ICT systems/applications under the Loss of IT section which means the details of arrangements the service has in place if this system is not available has not been recorded and the back-up storage information for this system has not been recorded. This is a cloud hosted system, but a copy of the cloud providers BC plan has not been obtained and referenced in the BC plan.
Action Description	The BC plan should be reviewed and updated to ensure the response team members are current staff members. The Flexiroute system should be listed at the Loss of IT section to ensure the details of arrangements the service has in place if this system is not available is recorded. The cloud provider should be contacted to obtain a copy of their BC plan and this should be referenced in this BC plan.
Risk	Non-compliance with the BC strategy; new critical processes have not been identified and documented; inaccurate or out of date information could delay the response during an incident.
Priority (1, 2, 3)	2
Paragraph Reference	3.18
Managed by	Gordon Mitchell, Senior Manager (Transport)
Assigned to	Susan Adamson, Team Manager (Journeys & Hires /Transport)
Due Date	Completed
Management Comment	The Business Continuity Plan has been reviewed and updated which has been communicated and is reflective of our current staffing structure. The Flexiroute system is now listed under the Loss of IT section of the Business Continuity Plan to ensure the details of arrangements are in place if the team were to experience a Flexiroute system failure. The system and cloud supplier (RLDatix) has provided a copy of their BC plan and this is referenced in the teams Business Continuity Plan.

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.

AGD – REVENUE PROJECTS

1 Background

1.1 The Ayrshire Growth Deal consists of a programme of 19 high-profile major development projects across Ayrshire involving public, private and 3rd sector partners and attracting funding from both Scottish and UK governments. East Ayrshire Council acts as the lead partner for the deal overall and hosts the Project Management Office (PMO). North Ayrshire Council is the lead partner for 9/19 of the projects (6 capital, 3 revenue).

1.2 The 3 Revenue Projects are Ayrshire-Wide but NAC is the lead partner for all of them. They are Community Wealth Building (CWB), Working for a Healthy Economy (WfHE) and Ayrshire Skills Investment Fund (ASIF).

1.3 The 3 projects are at very different stages. ASIF has only relatively recently received Final Business Case approval. Proposals include an employer grants programme. WfHE is largely undertaken by a contractor, NHS Salus, so the role of NAC is mostly of contract management. CWB was due to complete in March 2024, but an extension to March 2025 has recently been approved by the Ayrshire Economic Joint Committee.

2 Objectives and Scope

2.1 The audit was structured as 3 mini-audits covering each of the revenue projects, reflecting the different stages each audit had reached and the different natures of the projects.

2.2 The main objectives of the audit were to:

- Ensure that controls within the management of the Community Wealth Building project are suitable and operating effectively.
- Ensure that controls to manage the contract for the delivery of Working for a Healthy Economy are suitable and operating effectively.
- Provide audit advice regarding the proposals for the Ayrshire Skills Investment Fund, including an employer grants scheme.

2.3 Activities undertaken by East and South Ayrshire Councils as part of these projects were not audited directly, although the audit reviewed assurances obtained by NAC in relation to activities at East and South.

3 Findings

Community Wealth Building

3.1 Overarching governance is provided by an AGD CWB Programme Steering Group comprising representatives of the 3 Ayrshire local authorities. Performance and financial monitoring reports are regularly updated and submitted to the PMO. East and South Ayrshire Councils invoice North Ayrshire quarterly to cover their share of the staff costs and business grants that they have

distributed. A risk register is kept in the Ideagen (formerly Pentana) system and was updated during the audit period.

3.2 A sample of 10 grants to businesses was checked and overall the applications were all in order. They were paid by payment request and the required proof of bank details was not provided in 1 case or was inadequate in 4 further cases. The Business Support team, who process these claims, and the eProcurement team were advised to ensure that suitable proof of bank details is included in the payment requests. No other issues were identified.

3.3 The 5 "top deliverable" performance indicators were checked to ensure that suitable backup was available. All were found to be suitable. One of these indicators is called "CWB Officers and Action Plans in Place" and is calculated by adding together the number of officers in place and the number of action plans. It seems somewhat incongruous that these 2 figures are added together to form a performance indicator. North Ayrshire have contacted the PMO to query this methodology.

Working for a Health Economy

3.4 This project is provided by a contractor appointed in a procurement exercise. There is a service level agreement and the agreed costs are invoiced monthly by the contractor.

3.5 There is a steering group where the partner organisations and the contractor meet to discuss the progress on the project and any issues encountered. However, the steering group has not met regularly or, in some cases, meetings have taken place but minutes have not been produced. **(Action a)**

3.6 Performance data on people accessing support from this project are provided by the contractor and reported to the PMO. There is a risk register which has been updated as the project progressed.

Ayrshire Skills Investment Fund

3.7 The ASIF project was at an early stage at the time of the audit. The first round of grants to businesses was awarded in November 2023 and a second round was awarded near the end of the audit in February 2024.

3.8 The Grant Offer Letter remitted to grant recipients outlines requirements for grant recipients, including record keeping and accounting requirements. The businesses are required to sign and return a copy of the Grant Offer Letter.

3.9 Since the UK left the EU the State Aid requirements have been replaced with Minimum Financial Assistance requirements. Processes have been introduced to ensure that the grant recipients comply with these requirements.

3.10 A small sample of grants awarded in November 2023 was checked and all was found to be in order.

3.11 The service requested some advice regarding evidence requirements for the business grants. They had been asking for invoices for external training and for

training plans and hourly rates for in-house training. Furthermore, they make contact with all training recipients for monitoring and evaluation purposes, during and after the training. It was suggested that if the trainees do not engage adequately to demonstrate that the training has taken place, then further evidence should be requested from the businesses.

4 Internal Audit Opinion

4.1 Overall, substantial assurance was obtained with regard to the AGD Revenue Projects. The WfHE Steering Group meetings need to take place regularly and minutes be produced promptly after each meeting.

Definitions of Assurance Levels:

Substantial	A sound system of governance, risk management and control exist, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
None	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.

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

KEY FINDINGS AND ACTION PLAN
AGD – REVENUE PROJECTS

Action	a
Finding	The WfHE Steering Group has not met regularly or in some cases meetings have taken place but minutes have not been produced.
Action Description	The Employability team should ensure that WfHE Steering Group meets regularly and minutes of the meetings are produced in a timely manner
Risk	Issues with the project are not identified promptly. Agreed actions from the meetings are not implemented promptly. Different parties taking part in the meeting have a different understanding of what was agreed.
Priority (1, 2, 3)	2
Paragraph Reference	3.5
Managed by	Louise Kirk, Head of Service (Economic Development Growth and Regeneration)
Assigned to	Laura Neill, Senior Manager (Employability and Skills)
Due Date	6 June 2024
Management Comment	The issue has partly been addressed through a schedule of meeting dates which have been agreed with partners every 6 weeks. The next meeting is 30 May 2024. The next stage will be to ensure that an agenda is prepared at least one week in advance and the meeting minutes issued one week after the meeting date. This will be reviewed on 6 June 2024 to ensure compliance with the identified timescales and the action can be closed thereafter.

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.