NORTH AYRSHIRE COUNCIL

25 January 2024

Audit and Scrutiny Committee

Title:	**Internal Audit Reports Issued**
Purpose:	To inform the Committee of the findings of Internal Audit work completed between November and December 2023.
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 November and December 2023. 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 two 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
Employee Services HR Payroll System and Processes	Payroll Administration – Reasonable Service Administration – Limited
ICT Supplier Management	Reasonable

2.4 With regard to the HR Payroll review, limited assurance was provided around operational service administration. This is as a result of errors identified in the recording of absence information by services, as well as the volume of overpayments and manual corrections made by Employee Services as a result of delayed payroll notifications from services. Testing was carried out across all services, and as there was no pattern or particular services identified where this is causing an issue, an action has been raised for Employee Services to issue reminders generally to all services to ensure the timely and accurate provision of information. Automated process are being implemented to assist with these weaknesses, including weekly absence reports to help highlight where there may be errors in the recording of absence, and regular reporting to Heads of Service to highlight overpayments in their service areas.

3. Proposals

3.1 It is proposed that the Committee considers the outcomes from the Internal Audit work completed between November and December 2023.

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 the 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.

EMPLOYEE SERVICES - HR/PAYROLL SYSTEM AND PROCESSES

1 Background

1.1 CHRIS21 is the HR Payroll system used by North Ayrshire Council. The software is supplied by Frontier.

1.2 Regular payroll transaction testing is carried out annually, therefore these have been omitted from this audit.

1.3 Employee Services are responsible for running payruns based on information provided by Services. The onus is for managers to provide Payroll with timely and accurate information and it is employees' responsibility to ensure that they have been paid the correct amount.

1.4 As of October 2023, there were 7,584 employees on the payroll system.

2 Objectives and Scope

2.1 The objective of this audit was to establish:

- coverage of CHRIS 21
- contract details of service levels and data protection
- segregation of duties and access controls
- security of sensitive data, and
- ensure change requests are timely and accurate.

3 Findings

COVERAGE

3.1 There are nine modules currently in use within the HR Payroll system. These relate to HR information, payroll, fleet management, self-service and Public Sector returns.

3.2 Every NAC employee with corporate IT access has access to their own basic information and their payslip via the HR21 self-service module. Employees without IT access submit requests in writing by either email or post.

CONTRACT

3.3 The Frontier system was upgraded in November 2018. Due to the complex nature of the Council's Terms and Conditions of employment, there are few alternative software providers who provide a capable and affordable system. As a result, there is no plan to replace the HR Payroll system at this time.

3.4 The contract is listed on the Licences Subscriptions Software Support Register (LSSS Register). LSSS contract referencing is no longer used in procurement, however at the time the Contract was placed on the Register, this was acceptable. A STAR will be required to remove the Contract from the Register, and this is currently being completed by the Service. **(Action a)**

3.5 There are 19 Frontier invoices on Integra related to the CHRIS 21 system covering training, maintenance and consultancy costs. Maintenance costs are linked to the Retail Price Index (RPI) either at 2% or the actual if higher. Maintenance costs have increased from 3 years at 2% to 5% for the year ending 2023, and 10% for year ending 2024. With current inflation fluctuations this cost will continue to increase.

ACCESS CONTROLS AND SECURITY

3.6 At the time of the audit there were 475 CHRIS users with access to the HR21 self-service module, where they can view their payslips and P60's .

3.7 Policies and user guidance on the different CHRIS modules are available on Connects. A user guide for the HR21 self-service module is available via the HR21 homepage.

3.8 IT CHRIS user report analysis identified two security levels: level 5 'all other staff', and level 9 'executive staff' with a default user allocation of level 5. This is to ensure that there is an appropriate hierarchal access control to system records. There are 865 forms available on CHRIS; at the time of the audit it was confirmed that the Workforce Systems team are creating a screen tracker document to allow them to track what screens are in use. The purpose of this development is to enhance system security, eradicate screen duplication, support customisation requests, and ensure only active screens are within user profiles.

3.9 During the audit the software provider issued an update to user passwords to strengthen security controls. The new password settings are compliant with the Council's password configuration standards.

3.10 Access is assigned based on job roles, however there are two generic logins that could not be matched with active employees. **(Action b)**

CHANGE REQUESTS

3.11 Contractual changes are undertaken solely by the Employee Services team within CHRIS.

3.12 Employees with access to HR21 can update personal information such as home address, emergency contact and bank details directly. Employees without IT access are required to place their request in writing via email or by post to the Employee Services team.

3.13 Absences are recorded within the HR Payroll System. Managers are required to complete an online form which is routed to either the Employee Services team, (Place and Chief Executives) or the relevant Service admin team. Audit testing of a sample of absence records identified errors in dates such as incorrect start of the sickness absence and incomplete return dates. **(Action c)**

3.14 Employee Services track and manage absence related amendments through system reports.

3.15 There were 220 overpayments recorded in 2022/23 financial year with a recorded value of £231,780. The main cause of overpayments is late information relating to sickness absence, termination of employment and contractual changes. As a result, debtors invoices are raised and other retrieval costs are incurred by NAC. From a sample of 10 overpayments, 6 were due to late notification by the Service and a further 4 by clerical errors from the Service. Carrying out pay corrections can be resource intensive for the Payroll team and can require escalation to senior team members to seek advice and guidance on the best approach where cases are complex. In addition to the impact to the Payroll team, additional teams with Financial Management are required to take action. From the sample 1 case required 3 Employee Service staff to intervene. **(Action d)**

3.17 As a result of incorrect information being provided, the Employee Services team require to process supplementary payments to employees where contractual earnings have not been received. For the financial year 2022/23 there were 417 supplementary payments produced with a value of £327,033.

3.18 A cross service sample of 26 supplementary payments identified that 10 were because of the Service not completing the employee absence records. A further 9 were new start pay advances, which can be requested as a support when starting a new job and are recovered over their next 2 pays. In 1 case there was a software error which is being monitored, 2 were Service errors and 4 were Employee Services errors, which after review resulted in changes of procedure to prevent reoccurrence.

3.19 The administration of these payroll corrections is time consuming and labour intensive. On average the samples tested took 17 days to resolve, dependent on how quickly information is returned - a complicated maternity correction taking 58 days to resolve required 5 employee services staff's intervention. **(Action d)**

4 Internal Audit Opinion

4.1 Overall, reasonable assurance was obtained with regard to administration of payroll processes. Where issues have been identified processes have been amended to mitigate risks.

Limited assurance was obtained to the timely administration by services to provide accurate and timeous information to ensure the efficient and accurate payroll runs.

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
EMPLOYEE SERVICES - HR/PAYROLL SYSTEM AND PROCESSES

Action	a
Finding	A STAR is required to remove the Contract from the, now out of date, LSSS Register.
Action Description	Complete a Single Tender Action Request (STAR) and provided to the Procurement Team.
Risk	Continued use of this programme is non-compliant with NAC procurement standards.
Priority (1, 2, 3)	1
Paragraph Reference	3.4
Managed by	Fiona Walker, Head of Service (People and ICT)
Assigned to	Jackie Hamilton
Due Date	31/03/2024
Management Comment	A STAR is currently being prepared to remove the Contact from the LSSS register and ensure a contractual arrangement is in place with Frontier for another term.

Action	b
Finding	Generic accounts unassigned to individuals were identified.
Action Description	Investigate generic accounts and ascertain requirement for them to continue. Ensure Frontier user account is compliant with NAC identification processes.
Risk	Noncompliance with the Council's IT and GDPR policies.
Priority (1, 2, 3)	2
Paragraph Reference	3.10
Managed by	Fiona Walker, Head of Service (People and ICT)
Assigned to	Jackie Hamilton
Due Date	Complete
Management Comment	There are two generic logon IDs, which are required by both the Software provider and the Payroll Team. The Software provider's logon ID is locked unless they request access to it. The Payroll Team's logon on ID is view only to allow them to interrogate payroll records for previous financial years. A generic view only logon ID is used to avoid any corruption to the historical data. Based on the purpose of these logons there is limited risk to the Council's IT and GDPR policies.

Action	c
Finding	Inaccurate absence information recorded on CHRIS
Action Description	Managers should be reminded of the requirement to record absences completely and accurately.
Risk	Pay entitlements may be impacted by erroneous information resulting in both over and under payments of earnings. Additional officer time processing corrections.
Priority (1, 2, 3)	1
Paragraph Reference	3.13
Managed by	Fiona Walker, Head of Service (People and ICT)
Assigned to	Jackie Hamilton
Due Date	Complete
Management Comment	Senior Managers & Heads of Service are issued with an automated report on a weekly basis providing details of absences within their area. Senior Managers should review the data within the report and where they identify any issues advise the relevant admin team of required correction. The Employee Service team have created a report to check for errors in dates entered within the HR Payroll System. The report is run on a weekly basis, where discrepancies are found the error will be directed to the relevant service responsible for data entry to correct.

Action	d
Finding	637 payroll overpayments and manual corrections, with a value of £558,813, were identified by Employee Services in the 2022/23 financial year.
Action Description	Employee Services should use information records to report to Heads of Service on performance annually/bi-annually to improve standard of payroll notifications.
Risk	• Overpayments are incurred and not recovered. • Additional time is required to correct errors, including complicated manual calculations • Additional recovery costs are incurred.
Priority (1, 2, 3)	1
Paragraph Reference	3.15 and 3.19
Managed by	Fiona Walker, Head of Service (People and ICT)
Assigned to	Jackie Hamilton
Due Date	31/3/2024
Management Comment	A screen is being developed in the HR Payroll system to record details of overpayments (currently recorded within a spreadsheet). This development will allow for an automated report to be issued to Heads of Service on a 6-monthly basis providing details of overpayments within their Service including the reason and amount. Heads of Services will be advised in advance of this process commencing and requested to reinforce the importance to their managers of submitting timely and accurate information.

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.

ICT SUPPLIER MANAGEMENT

1 Background

1.1 The audit program was based on the Public Sector Cyber Resilience Framework refresh document. Section 3 of this framework covers Supplier Management, the main objective being to ensure the Council understands and manages security risks that arise as a result of dependencies on external suppliers and third party services.

1.2 The audit included 3rd party suppliers that IT Services are responsible for managing and also a small sample of recent contracts for cloud-based systems.

1.3 The audit involved testing within IT Services and Procurement.

1.4 The Procurement Manual provides clarity on how NAC should procure its goods, works and services to ensure best value is achieved. The manual must be used by all staff involved in the Procurement process. A list of NAC contracts and framework agreements are detailed within NAC's corporate contract register. A framework agreement is a general term for agreements with suppliers that set out terms and conditions under which specific purchases (call-offs) can be made throughout the term of the agreement.

1.5 The Senior Manager (Corporate Procurement) advised a Terms and Conditions of Contract for Information Communication Technology (ICT) Services has recently been finalised and is now available on the Conditions of Contract Procurement page of Connects. This is based on the Scottish Government ICT Terms and Conditions.

2 Objectives and Scope

2.1 The objectives of the audit were to ensure that:

- The Council has defined the respective duties and responsibilities of third-party suppliers and the supply chain and these are understood and agreed by all parties.
- There is visibility and control on third-party users that can access Council systems, services and information data and these are appropriately verified, authenticated and authorised.
- The Council has security embedded within procurement procedures.
- The Council has security embedded in cloud-based services.

2.2 The supply chain assurance section of the Cyber Resilience Framework for ICT Supplier Management will be included in an upcoming Business Continuity audit.

3 Findings

Roles and Responsibilities

3.1 The Terms and Conditions of Contract for ICT Services has recently been finalised and is now available on the Conditions of Contract Procurement page of Connects. This will be issued for all relevant contracts involving ICT Services that are not part of a framework agreement. The Terms and Conditions of Contract for ICT Services is based on the Scottish Government ICT Terms and Conditions and adequately covers the requirements of the cyber resilience framework for ensuring the roles and responsibilities of each party are included as part of the contract.

Access Control

3.2 During the audit, IT Services updated their documented process for third parties requiring temporary access to Council systems and servers to support our IT operations. This access is granted via a Virtual Private Network (VPN) connection which needs to be set up by IT Services. Access is restricted to the minimum access necessary. Once set up the third party will need to request the VPN connection is opened and unless additional time is requested, the connection will be automatically closed at 6pm the same day. VPN connections are decommissioned when no longer required. All such requests are now on Hornbill, the IT Services Portal.

3.3 The initial request to set up a VPN connection requires the third party to sign the third Party Acceptable Use Policy. IT Services provided a list of current VPN third party users and advised most of them were historically set up and may not be able to provide evidence they have signed the 3rd party Acceptable Use Policy (AUP). Internal Audit and IT Services agreed that all current suppliers on the VPN list would be asked to sign up to the third party AUP to ensure this evidence was up to date and available. A Microsoft Form is now completed for such purposes which provides an electronic audit trail of who has signed this form and when. There are 29 suppliers on the VPN list and 11 of them have at least 1 user that has signed this policy and 18 of them have no users that have signed this policy. IT Services are actively chasing suppliers to ensure their users sign up to the third party AUP.

3.4 There are a number of non-Council employees that require permanent access to the Council network and systems and as such, an active directory account is set up which grants network access. A request to set up an active directory account is logged on Hornbill and the Hornbill reference number is logged against the active directory account along with the email address of the person who requested the account to be set up. This ensures there is an adequate audit trail for such accounts.

3.5 IT Services advised that the relevant NAC manager is responsible for notifying when a non-NAC active directory account is no longer required. IT Services also have an automatic process in place to disable active directory accounts that have not been used within 90 days. IT Services provided an active directory report of all non-NAC users and their last logged on date. This testing found 1 Care at Home (CAH) user who only has email on a mobile phone and never logs onto a NAC device that has not used their email within the last 90 days. IT Services are looking into an automated process to remove CAH leavers.

Security in Procurement

3.6 The auditor reviewed the Procurement Manual which specifies which procurement process to follow depending on the procurement value. Although it covers procurement exercises that are below an estimated contract value of £10,000, the Procurement Manual does not refer to the Information Governance Procurement Framework (IGPF) for such low value procurements to ensure information governance and IT, cyber and information security requirements are considered. **(action a)**

3.7 For procurement exercises that are above an estimated contracted value of £10,000, the Procurement Manual requires a Request for Procurement Action (RPA) form to be completed. Section 5 of the RPA incorporates the Information Governance and ICT Security requirements of the IGPF. If Information Governance implications are identified, the IGPF must be completed. If ICT security implications are identified, an IT, Cyber and Information Security Schedule should be included in the procurement exercise. This schedule ensures the supplier declares compliance with baseline security standards and obligations. If the supplier has identified any areas of non-compliance, the Council's ICT Security Officer will undertake a risk assessment where detailed mitigating controls and evidence have been provided.

3.8 There is no version control on the IGPF so it is unclear when it was last updated. Although it is called the Information Governance Procurement Framework, section 1 covers Information Governance, section 2 covers IT, Cyber and Information Security and section 3 covers Information Technology Considerations so the title does not refer to the ICT cyber security considerations. The IGPF should be reviewed in consultation with Corporate Procurement and updated to ensure it is still fit for purpose. This update should incorporate who to contact for help or advice when completing this framework. Consideration should also be given to renaming the framework. **(action b)**

3.9 There is a risk that services purchasing IT related services and data hosting solutions as well as enhancements or upgrades to existing provisions do not follow the proper procurement process and the IGPF is not followed which could result in information governance and IT, Cyber and Information Security requirements not being considered. As more IT systems move to cloud-based services, there is a greater need to consider information governance and ICT cyber security requirements. The IGPF is only available on the Procurement pages of Connects and is not included in the IT Services or Information Governance Connects pages. Once the IGPF is refreshed, services should be reminded that for all purchases, regardless of value, there is a requirement to complete the IGPF. Internal Audit recommends this should be done via News in Brief and a MetaCompliance message. **(action c)**

3.10 Information Governance advised they started a review of the IGPF in October 2023 which will review the current process by removing duplication and adding further guidance to signpost services to the relevant teams, contacts and processes. An action plan has been produced after an initial meeting with Procurement. The findings of this audit will be incorporated into this review.

3.11 There were 2 IT contracts selected for audit testing and neither had a completed IT, Cyber and Information Security Schedule in the Procurement folder. The Information Governance Procurement Framework states "where a supplier has not received this schedule as part of a procurement exercise it may be included within the contractual arrangements." Both contracts were mini competitions from the Crown Commercial Services Frameworks and IT Services and Procurement advised that IT security requirements were included within the contractual arrangements and this schedule was not required. Although the proper procurement process was followed, there was no evidence in the Procurement folder to note why this schedule was not included in the tender documentation. It is recommended the IGPF checklist is updated to include a section to record where the IT, Cyber and Information Security Schedule is not required and the reason for this. **(action b)**

Security in Cloud Services

3.12 The auditor selected 2 contracts for the provision of cloud-based systems, and both were a Crown Commercial Service G-Cloud 13 Call-Off Contract. The supplier had completed the IT Cyber Information Security Schedule which confirmed compliance with the NCSC's 14 principles of the Cyber Security Requirements for Cloud Service providers. In addition, the call-off contract ensures compliance with the same cloud security principles.

3.13 The Public Sector Cyber Resilience Framework recommends the Cloud Service Provider should specify and document the physical geographic locations of data, including any locations in which data is processed or backed up. It should be noted that the 2 call-off contracts in the sample do not record the location of the data being processed and backed up in the contract documentation. **(action b)**

4 Internal Audit Opinion

4.1 Overall, reasonable assurance was obtained with regard to the testing carried out for ICT supplier management. The biggest risk is the Information Governance Framework not being followed which could result in data security and ICT cyber security requirements not being considered. Implementation of the audit actions should strengthen the controls around this 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
ICT SUPPLIER MANAGEMENT

Action	a
Finding	The Procurement Manual does not refer to the Information Governance Procurement Framework (IGPF) for procurements with an estimated value of under £10,000 to ensure information governance and IT, cyber and information security requirements are considered.
Action Description	Once the IGPF has been updated, the Procurement manual should be updated to signpost the refreshed framework for all procurements, the RPA should be updated to reflect the refreshed framework and the Procurement page on Connects should be updated to signpost the refreshed framework for all purchases regardless of value.
Risk	Data security and ICT cyber security requirements have not been considered which could result in a data breach or a cyber security breach.
Priority (1, 2, 3)	2
Paragraph Reference	3.6
Managed by	Mark Boyd, Head of Service (Finance)
Assigned to	Suzanne Quinn, Senior Manager (Corporate Procurement)
Due Date	07/05/24
Management Comment	The Corporate Procurement Unit will update The Procurement Manual, RPA and relevant information on the procurement Connects page to refer to the updated IGPF one week after the IGPF has been refreshed.

Action	b
Finding	There is no version control on the IGPF so it is unclear when it was last updated. Although it is called the Information Governance Procurement Framework, section 1 covers Information Governance, section 2 covers IT, Cyber and Information Security and section 3 covers Information Technology Considerations, so the title does not refer to the ICT cyber security considerations. The Public Sector Cyber Resilience Framework recommends the Cloud Service Provider should specify and document the physical geographical location of data, including any locations in which data is processed or backed up. It should be noted that the 2 call-off contracts in the sample do not record the location of the data being processed and backed up.
Action Description	The IGPF should be reviewed in consultation with Corporate Procurement and updated to ensure it is still fit for purpose. This update should incorporate who to contact for help or advice when completing this framework. The update should also prompt the user to only consider suppliers where the geographical location is compliant with GDPR regulations of data and ensure this information is captured during the procurement process. Consideration should also be given to renaming the framework. The IGPF checklist should be

	updated to include a reason if the IT, Cyber and Information Security Schedule is not required.
Risk	Services do not know who to contact for advice from the experts. The jurisdiction where the data is stored is not known and may not have adequate protections for personal data.
Priority (1, 2, 3)	2
Paragraph Reference	3.8, 3.11, 3.13
Managed by	Aileen Craig, Head of Service (Democratic) and Fiona Walker, Head of Service (People & ICT)
Assigned to	Brendan Quigley, Senior Manager (IT Services) and Lauren Lewis, Information Governance & Data Protection Manager
Due Date	30/04/2024
Management Comment	IT Services and Information Governance will work together with the Corporate Procurement Unit to review and update the IGPF.

Action	c
Finding	There is a risk that services purchasing IT related services and data hosting solutions as well as enhancements or upgrades to existing provisions do not follow the proper procurement process and the IGPF is not followed which could result in information governance and IT, Cyber and Information Security requirements not being considered. As more IT systems move to cloud-based services, there is a greater need to consider information governance and ICT cyber security requirements. The IGPF is only available on the Procurement pages of Connects and is not included in the IT Services or Information Governance Connects pages.
Action Description	Once the IGPF is refreshed, services should be reminded that for all purchases, regardless of value, there is a requirement to complete the IGPF. Internal Audit recommends this could be done via News in Brief and a MetaCompliance message. In addition, a link to the IGPF should be added to the IT Services and Information Governance pages on Connects.
Risk	Data security and ICT cyber security requirements have not been considered which could result in a data breach or a cyber security breach.
Priority (1, 2, 3)	2
Paragraph Reference	3.9
Managed by	Aileen Craig, Head of Service (Democratic) and Fiona Walker, Head of Service (People & ICT)
Assigned to	Brendan Quigley, Senior Manager (IT Services) and Lauren Lewis, Information Governance & Data Protection Manager
Due Date	30/04/2024
Management Comment	IT Services and Information Governance will work together with the Corporate Procurement Unit to issue communication in relation to the updated IGPF and to remind services that the IGPF should be completed for all purchases, regardless of value.

	A link to the IGPF will be added to the IT Services and Information Governance pages on Connects.

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.