

To: Audit, Risk and Scrutiny Board

On: 24 August 2020

Report by: Chief Auditor

Heading: Summary of Internal Audit Reports for period 01 January to 30 June 2020

1. Summary

1.1 In line with the Public Sector Internal Audit Standards, Internal Audit must communicate the results of each engagement to the Board. To comply with this requirement Internal Audit submits regular reports on the findings and conclusions of audit engagements to the Audit, Risk and Scrutiny Board.

1.2 Appendix 1 provides details those audit engagements completed during the period 01 January to 30 June 2020 with the overall assurance rating and the number of recommendations in each risk category. The committee summary for each report is also attached. For each audit assignment where recommendations have been made, the relevant managers have put action plans in place to address the issues raised.

1.3 In addition to the reports listed in the Appendix, Internal Audit has an ongoing commitment to:

- A range of corporate and service initiatives;
- Progressing of information security matters in partnership with ICT and Legal Services;
- The regular provision of advice to departmental officers;
- The provision of internal audit services to the associated bodies for which Renfrewshire Council is the lead authority and to Renfrewshire Leisure Ltd and Renfrewshire Health and Social Care Integrated Joint Board;

- Co-ordination of the Council's corporate risk management activity;
 - Management of the counter fraud team;
 - Management of the risk management and insurance team.
-

2. **Recommendations**

- 2.1 Members are invited to consider and note the Summary of Audit Reports finalised during the period from 01 January to 30 June 2020.
-

Implications of the Report

1. **Financial** - None
2. **HR & Organisational Development** - None
3. **Community Planning – Safer and Stronger** - effective internal audit is an important element of good corporate governance.
4. **Legal** - None
5. **Property/Assets** - None
6. **Information Technology** - None
7. **Equality & Human Rights** – None
8. **Health & Safety** – None
9. **Procurement** - None
10. **Risk** - The summary reported relates to the delivery of the risk-based internal audit plan.
11. **Privacy Impact** – None
12. **COSLA Implications** – None
13. **Climate Risk** - None

Author: Karen Campbell – 07768354651

Appendix 1

Renfrewshire Council

Internal Audit Service

Update for Audit, Risk and Scrutiny Board

Final Audit Reports issued from 01 January – 30 June 2020

Category	Service	Engagement	Assurance Rating	Recommendation Ratings			
				Critical	Important	Good Practice	Service Improvement
Assurance	FAR	ICT Monitoring – Payment Card Industry Standards	Limited	0	5	3	0
	FAR	General Ledger Processes	Reasonable	0	2	2	1
	FAR/Adult Services	Corporate System Access	Reasonable	0	2	2	1
	Children's Services	Fostering & Kinship - Payments	Reasonable	0	2	2	0
Governance	Adult Services	Information Security	Reasonable	0	2	2	0
Investigation	Environment & Infrastructure	Atrium Card Payment Variances	N/A	0	3	1	0

Note 1 – No assurance rating can be given in respect of investigation assignments

Assurance Level	
Substantial Assurance	<ul style="list-style-type: none"> • There is a sound system of internal control designed to achieve the objectives of the area being reviewed. • The control processes tested are being consistently applied.
Reasonable Assurance	<ul style="list-style-type: none"> • The internal control processes are generally satisfactory with some areas of weakness being identified that could put some objectives of the area being reviewed at risk • There is evidence that the level of non-compliance with some of the control processes may put some of the objectives of the area being reviewed at risk.
Limited Assurance	<ul style="list-style-type: none"> • Weaknesses in the system of internal controls are such as to put the objectives of the area being reviewed at risk. • The level of non-compliance puts the objectives of the area being reviewed at risk.
No Assurance	<ul style="list-style-type: none"> • Control processes are generally weak with significant risk to the achievement of the objectives of the area being reviewed. • Significant non-compliance with control processes leaves the processes/systems open to error or abuse.

Recommendation Rating	
Service Improvement	Implementation will improve the efficiency / housekeeping of the area under review.
Good Practice	Implementation will contribute to the general effectiveness of control.
Important	Implementation will raise the level of assurance provided by the control system to acceptable levels.
Critical	Addresses a significant risk, impacting on the objectives of the area under review.

Internal Audit Report

Finance and Resources

ICT - Payment Card Industry Standards (A0075/2020/001)

Date: June 2020

COMMITTEE SUMMARY

Audit Objectives
<p>The objectives of this audit are to ensure that:</p> <ol style="list-style-type: none"> 1. Supervisors train staff in how to check that chip and pin devices have not been tampered with and this training is renewed annually. 2. Retained cardholder data is the absolute minimum necessary. 3. Merchant receipts are stored in a secure area and are clearly marked with their scheduled due destruction date. 4. The retention policy for Merchant receipts retained in a digital and paper format is being followed. 5. Card handling staff concerns are appropriately escalated to the appropriate Council Officers 6. Installation, maintenance, replacement and return of devices is done with assistance and verification of ICT Services. 7. Leaver accounts are deactivated and long term absence accounts rendered inactive. 8.
Audit Scope
<p>The following work was carried out:</p> <ol style="list-style-type: none"> 1. Following discussion with the Cyber Security Architect the focus of the audit was to test compliance with the PCI Compliance Policy for Card Handling Teams. 2. We selected a sample of council teams who process credit and debit card payments using Chip and Pin machines and tested that they comply with the requirements of the policy. We did not test payments made on the internet, by telephone or using kiosks.
Key Audit Assurances
<ol style="list-style-type: none"> 1. At the locations visited, retained cardholder data was kept to the minimum necessary. 2. Merchant receipts were securely stored and filed in date order.
Key Audit Risks
<p>If staff are not regularly made aware of Card Handling and Chip and Pin Device Tampering policies, they may not carry out instructions in these policies to the required standard.</p>

Internal Audit Report

Finance and Resources

ICT - Payment Card Industry Standards (A0075/2020/001)

Date: June 2020

Overall Audit Opinion

The audit has shown that retained cardholder data was appropriate and merchant receipts were securely stored. Some recommendations have been made including to regularly make staff aware of Card Handling procedures and to inform IT of any changes to card payment equipment. If implemented, these actions will enable staff to fully comply with Payment Card Industry Data Security Standards (PCI DSS).

Management Commentary

Management are implementing the recommendations made by updating their procedural manuals and arranging refresher training programmes for the staff involved in processing card payments. Daily control sheets have been introduced to confirm chip and pin machines have been checked for tampering.

Procedures have been implemented to ensure that Services are aware of the need to inform ICT/Cyber Security if any proposed card payment equipment changes. The Cyber Security team will then assess and advise on the suitability of the proposed equipment to ensure it aligns with PCI requirements.

Internal Audit Report
Finance and Resources
General Ledger Processes (A0080/2020/001)

Date: May 2020

COMMITTEE SUMMARY

Audit Objectives

The objectives of the audit were to ensure that:

1. Adequate controls have been established to protect information and data from unauthorised access.
2. Coding Structures are being adhered to and strictly controlled with transactions being correctly coded and recorded.
3. The Policies and procedures detail the accounting procedures to be followed and are available to all necessary staff.
4. Journals and Internal Transactions are appropriately authorised and recorded.

Audit Scope

The following work was carried out:

1. Obtained the current policies, procedures, Business World staff guidance and coding structure and assessed for adequacy.
2. Interviewed the appropriate members of staff to ascertain the processes for journals.
3. Prepared a programme of tests covering these areas.

Key Audit Assurances

1. The Business World ledger staff guidance provides comprehensive instructions for individual tasks.

Key Audit Risks

1. Where password controls are not completely operational, there is a risk that Business World information is not fully protected from unauthorised access.

Overall Audit Opinion

The Business World ledger staff guidance was found to be satisfactory. Recommendations have been made within the report to strengthen the controls surrounding general ledger password access, transaction coding and journal entry authorisation.

Internal Audit Report
Finance and Resources
General Ledger Processes (A0080/2020/001)

Date: May 2020

Management Commentary
<p>The password policy within Business World has been amended in line with other Council Applications and ICT Guidance. Reminders will be sent to users of the system regarding accurate transaction coding and good practice to be followed when processing journals.</p> <p>The roles established for financial tasks are against the Business World Finance positions and this provides further security that only those identified to carry out certain tasks will be able to undertake these. The Business World Team have worked with the Finance service and understand that the system steps within the guidance available meets all their needs and requirements.</p>

Internal Audit Report
Finance and Resources/Adult Services
Corporate System Access (A0074/2019/002)

Date: March 2020

COMMITTEE SUMMARY

Audit Objectives

The objectives of the review were to ensure that in relation to SWIFT:

1. There is an adequate process in place to approve and allocate system access to Business Services employees.
2. Employees are made aware of and acknowledge their responsibilities in relation to systems access, particularly for systems containing sensitive or personal information.
3. There is a process in place to identify and remove access that is no longer required, including transfers, terminations and temporary cover arrangements.
4. Periodic checks are undertaken on system access to ensure that it is appropriate to the employees' role.
5. Administrator access is only granted where this is appropriate to the employees' role.
6. To establish the current processes in place for Business World in relation to the above objectives to enable future testing of the system.

Audit Scope

The following work was carried out:

1. Interviewed the appropriate officers to ascertain background information.
2. Established the current processes in respect of user access management for Business Services employees relative to the engagement objectives.
3. Obtained relevant information and undertook a programme of audit tests.

Key Audit Assurances

1. There is an adequate process in place to approve and allocate system access to Business Services employees through completion and authorisation of user access forms.
2. There is an e-learning course that employees should complete annually so that they have an up to date awareness of their responsibilities in relation to systems access.
3. Periodic checks are undertaken on access to SWIFT to ensure that it is appropriate to the employees' role.
4. There are no Business Services employees with inappropriate administrator access.
5. Processes are in place or are currently being established in relation to the above objectives for Business World.

Key Audit Risks

1. There could be financial and reputational risks to the council if employees with access to personal information are not familiar with the most up to date General Data Protection Regulations and Information Security protocols.

Internal Audit Report
Finance and Resources/Adult Services
Corporate System Access (A0074/2019/002) Date: March 2020

Overall Audit Opinion
There are processes in place to ensure that appropriate access is granted to employees aligned with their job role and to ensure that employees are made aware of their responsibilities in relation to information security. However, these could be improved upon and the auditor has made recommendations to increase the robustness of current controls. The auditor has therefore given a level of reasonable assurance in this area.

Management Commentary
Management have taken action to ensure all user access request forms are fully and accurately completed, and all employees complete the required training.

Internal Audit Report Childrens Services

Fostering & Kinship - Payments (A0098/2020/001) Date: February 2020

COMMITTEE SUMMARY

Audit Objectives

The objectives of the review were to ensure that:

1. Processes are in place to ensure that new carers have been appropriately approved and they are added timeously and accurately to the payment run;
2. There is evidence that all required review processes have been satisfactorily undertaken to ensure that correct payments continue to be processed;
3. Adequate and authorised documentation is retained to support discretionary payments made;
4. Processes are in place to ensure that when carers terminate they are removed from the payment run timeously and accurately.

Audit Scope

The following work was carried out:

1. Obtained details of relevant procedural and legislative guidance.
2. Following discussions with the appropriate officers, prepared a series of tests to meet the audit objectives. We did not test any adoption cases.

Key Audit Assurances

1. Adequate processes are in place to ensure that new carers have been added accurately to the payment run.
2. Suitable processes are in place to ensure that when carers finish, they are removed from the payment run timeously and accurately.

Key Audit Risks

1. Evidence of adequate documentation is not being retained in relation to authorising Foster Carers, Independent Foster Carers and Kinship Carers applications.
2. There is not adequate evidence that all required review processes have been satisfactorily undertaken for Kinship Carers.

Overall Audit Opinion

There were adequate processes in place to add new carers and to remove carers from payruns when they finish. However, the audit has identified that evidence of authorising Foster Carers, Independent Foster Carers and Kinship Carers applications are not always retained in the expected files. Evidence of approval of some Foster Carers invoices and reviews of Kinship Carers were also lacking. The auditor has made a provision of reasonable assurance in relation to the area under review.

Internal Audit Report Childrens Services

Fostering & Kinship - Payments (A0098/2020/001) **Date: February 2020**

Management Commentary
Management are implementing the recommendations made, including reminding the appropriate locality managers of the processes to be followed and ensuring all appropriate training is completed.

Internal Audit Report Adult Services

Information Security (B0010/2020/001)

Date: May 2020

COMMITTEE SUMMARY

Audit Objectives

The objectives of the review were to ensure that client information:

1. Is protected from unauthorised use and is securely stored when not in use;
2. Is archived in line with the council's Records Management Policy;
3. Arrangements are in place to ensure that Data Privacy Impact Assessments are undertaken when required;
4. Arrangements are in place to provide training on GDPR to relevant employees;
5. Procedures are in place to identify data breaches and report them to the council's Data Protection Officer

Audit Scope

The following work was carried out:

1. Ascertained the information that adult services hold, assessed the sensitivity of the information and how it is stored.
2. Selected a sample of two adult service's locations and discussed with appropriate staff the arrangements in place to demonstrate compliance with information security good practice.
3. Reviewed and assessed the evidence to support compliance and identify any possible improvements.
4. Adult Services records are required to be retained for the Scottish Historic Child Inquiry. Adult Services currently have an unlimited retention period and so the auditors did not test retention periods in line with council retention periods.

Key Audit Assurances

1. Arrangements are in place to ensure that Data Privacy Impact Assessments are undertaken when required.
2. Staff demonstrated good awareness of procedures to be followed in relation to information security incidents.

Key Audit Risks

1. When staff do not complete Data Protection and Information Governance ilearn modules and annual refresher training, they may not be aware of GDPR procedures.
2. When there are some staff with access to restricted folders which management were unaware of, there is a risk that staff may have access to information they should not have access to.

Internal Audit Report Adult Services

Information Security (B0010/2020/001)

Date: May 2020

Overall Audit Opinion

The audit review provided reasonable assurance over arrangements in place for security of Adult Service's client information. It is recommended that Adult Service's management take steps to significantly increase the number of officers completing Data Protection and Information Governance ilearn modules and annual refresher training and review access to restricted folders.

Management Commentary

RHSCP comply with the mandatory data protecting training and refresher training currently available via ilearn. All Renfrewshire Council staff working within the partnership are also mandated to review the SIRO bulletin and remain up to date in this area. The HSCP ensure that staff are not provided full operational access to social work systems unless data protection courses have been completed. User management process also cross reference with business world reporting to ensure all employees no longer working in social work are removed from the system.

In addition, the HSCP have recently worked with Information Governance colleagues to ensure the acceptable use policy is explicit in misuse e.g. accessing friends and family social work records. This friends and family revision is routinely circulated within the HSCP and additional consideration will be given to the use of iLearn to support the partnership in demonstrating all staff remain up to date and aware of SIRO instructions. In the meantime all staff are guided to the relevant intranet pages.

Internal Audit Report
Environment & Infrastructure
Atrium Card Payment Variances (C0003/2020/018) Date: March 2020

COMMITTEE SUMMARY

Audit Objectives

Treasury section staff brought variances between card payment amounts recorded at the Atrium café and card payment amounts shown in the ledger, which appeared to be outside the normal range, to the attention of Internal Audit. The objectives of the audit therefore were to:

1. Ascertain the circumstances surrounding variances between card payment amounts recorded at the Atrium café and card payment amounts shown in the ledger which appeared to be outside the normal range.
2. Ascertain the processes for cashing up and security of monies, identify any weaknesses and make recommendations for improvements where necessary.

Audit Scope

The following work was carried out:

1. Identified any control weaknesses, any non compliance with procedures and make recommendations for improvement where necessary.

Key Audit Assurances

1. The auditor was satisfied that variances tested were as a result of timing differences.

Key Audit Risks

1. Where one person counts cash by themselves, there is an increased risk of loss or errors.
2. Revised security arrangements over keys and cash is required to be considered by management.

Overall Audit Opinion

At the time of the review Atrium café staff were cashing up before the café closes and some cash and card payments are included in the next day's takings. Therefore, although it was established that most variances between card payments recorded in the café and recorded by the bank (in the ledger) are timing differences, it is advisable that tills should be cashed up after the café closes. Some other matters were identified by the auditor which should be addressed to improve controls in the cashing up and banking process.

Internal Audit Report
Environment & Infrastructure
Atrium Card Payment Variances (C0003/2020/018) **Date: March 2020**

Management Commentary
Management have amended working practices in order to implement the recommended audit actions with one exception. Following management consideration of the risk and the level of cash held overnight, for operational reasons no changes have been made to the security arrangements.