3(iii)(b)
(17/149)

Internal Audit Report
Housing & Community Safety
SWIFT System
Assignment No.16-04
March 2017

Final Report

Finance Division
Corporate and Democratic Services
Perth & Kinross Council
Council Offices
2 High Street
Perth
PH1 5PH

Internal Audit

"Internal Audit is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes". Public Sector Internal Auditing Standards (PSIAS)

On 27th March 2013, the Council's Audit Committee approved the PSIAS as the relevant standard for its Internal Audit activity.

Background and Introduction

This audit was carried out as part of the audit plan for 2016/17, which was approved by the Audit Committee on 30 March 2016.

The SWIFT system is used to manage Perth and Kinross Council (PKC) clients' information in the provision of Adult Care and Children's Services. SWIFT was first installed at PKC in 2005 and is currently used by 9 other Scottish local authorities. SWIFT can be accessed by other Council services staff including Housing, Adults Social Care and Children's Services teams and also third parties. The Swift system is managed by the Business Systems Team. Upgrades are also managed/co-ordinated by the Business Systems Team Leader. The supplier does the upgrades with support from the Business Systems Team and Corporate IT (who manage the infrastructure). PKC upgraded to the latest version of Swift in May 2016.

Scope and Limitations

The audit reviewed controls in place by interviewing relevant personnel and checking sample system documentation, relevant corporate guidance and procedures relating to the system and system data. Due to the size and complexity of the application, the scope of this review was limited to reliance on this evidence for testing. Online access to the system was not requested.

SWIFT system is used to manage Council clients' personal information. As such, it falls within legislative areas for the protection of personal data, i.e. the Data Protection Act and the incoming General Data Protection Regulation 2016. The Act and new Regulation carry large potential penalties for non-compliance by organisations. Effective management of SWIFT records can also deliver significant benefits for PKC, for example, demonstrate proper treatment of personal information and maintain confidence between PKC and its clients.

Key officers interviewed included the Business Improvement Manager for Housing & Community Safety, the Business Systems Team Leader as the System Responsible Officer, the IT Co-ordinator (Applications) and the Council's Information Compliance Manager during February 2017.

The audit did not review information sharing with third parties and areas already covered in audit 16-05 Information Sharing.

Control Objectives and Opinions

This section describes the purpose of the audit and summarises the results. A 'control objective' is a management objective that requires the maintenance of adequate and effective internal controls to ensure that it is achieved. Each control objective has been given a rating describing, on the basis of the audit work done, the actual strength of the internal controls found to be in place. Areas of good or poor practice are described where appropriate.

Control Objective 1: To ensure that support and maintenance arrangements are in place for the SWIFT system

Audit Comments: PKC has a 5 year contract agreement with the SWIFT software supplier up until the end of March 2019. There are regular meetings of the Scottish SWIFT End User Group, which is currently chaired by PKC's Business Systems Team Leader.

Corporate IT manages the hardware infrastructure that holds SWIFT data. Regular backup and restore tests are carried out for SWIFT data and confirmation reports sent to the Service Desk on completion. Policy and procedures for backup and restore test policy are documented. In the event of any system failure, recovery of data up to the last working day should be available through the process in place. The SWIFT system is categorised as the highest priority Council application on the Corporate IT current business continuity plan.

The SWIFT supplier advised that an end of support notice is planned for issue to customers in April 2017. Development is planned to cease for the SWIFT (Adult and Children) product after 31st March 2017. Support for the product is planned to end on 31 March 2020, including the recent Adult Integrated Services (AIS) and the Children's Case Management (CCM) products used by PKC practitioners. The supplier will make critical fixes as required until March 2020. To ascertain the way forward, a paper on the future of SWIFT has been produced by the Head of Revenues and Corporate IT advising relevant officers. The Scottish SWIFT End User Group has also requested the supplier to extend the 3 year notice to 5 years.

In addition, vulnerability was identified within SWIFT in November 2016. It was reported that work was underway to upgrade and fix this vulnerability during the audit and has now been fixed.

Strength of Internal Controls:	Moderate

Control Objective 2: To ensure that adequate physical and logical access controls are in place for SWIFT

Audit Comments:

<u>Access control and documentation</u>:

In line with good practice guidance in the Information Security Standard, ISO279002:2013, a Business Systems Access Control Policy document by Housing and Community Safety has been produced, dated 2015. This is understood to be due for review and update.

There is also a Business Systems Procedures Document, dated May 2015 which defines system administration procedures and access controls for SWIFT.

<u>SWIFT environments</u>: It was reported that the LIVE environment is used in place of a previous TRAIN environment for user training and that this is carried out under supervision. Thus, users can input and update live data during training, logged in

and recorded by their User ID.

Training: Users are also required to complete training by requesting this on a training request form. After training and login request forms are authorised by Line Managers, training and access is provided by the SWIFT Business Systems Team as required. Training guides are available for SWIFT users including -

Housing and Community Safety Generic AIS Personal Details Training Guide

AIS Adult Care Plans and Service Delivery User Guide

AIS and SWIFT - Adult Protection User Guide

Child Case Management [CCM] Helpful Hints and Tips

CCM Viewing the Electronic Social Care Record (ESCR)

There is also Council wide policy on clear desks as part of the flexible working arrangements for offices; staff are encouraged to lock or switch off their devices if there are leaving them. Devices automatically lock after a set period of time.

Access to SWIFT and password authentication: In advance of accessing SWIFT, users require written authorisation by their Manager. This was evidenced in a sample request form. Forms are sent to the SWIFT Team for processing. If SWIFT system user requests are agreed, the user is then provided with a username and first password on a written form via email. They are requested to sign their agreement to maintain confidentiality of information and their Line Manager has to countersign the same form. This form is then sent to PKC Employee Support Service and recorded on SWIFT as being completed. Therefore the first password and username is viewed by several staff during this process and held on their staff file. This does not comply with SWIFT Confidentiality and Passwords, Looking after Information – Staff Awareness guidance which requires usernames and passwords to be kept confidential and not shared.

Users are also required to sign a formal agreement reminding them of their obligations for confidentiality of information and the Council’s Employee Code of Conduct. Third parties accessing SWIFT are required to sign up to the same disciplinary treatment as PKC employees if they are found to break the confidentiality agreement.

It was reported that system administrators’ access allows them to input data as well as carry out administrative tasks.

There was a satisfactory detail of activated and de-activated user IDs listed dating back to 03/07/2009 which system administrators can view as required.

One generic login for Online Training set up in July 2012 was reported to not be in common use.

The option to force users to change their password was not switched on. However, prior to accessing SWIFT, users also have to access the PKC network, which has an enforced change of password every 40 days.

User management: To assist in user management, SWIFT administrators can interrogate and produce reports on User Groups and permissions in SWIFT as required. Sample reports were provided - all Member User-Groups and also for the new Launchpad Titles for AIS Users. The former listed 82 User Groups, of which 32 were ‘defaults’ and noted 1172 SWIFT users set up with these groups on 22

March 2017. Default groups were reported to be useful as templates from which to set up users' access by job requirements.

The process for identifying change to user access requirements has been reliant on Managers notifying the Business Systems Team, awareness of the SWIFT Business Systems Team of changes (for example through information in staff newsletters on staff who have left the Council) and through sending out requests to Team Leaders to regularly review lists of those with SWIFT systems access for the Business Systems Team. However, in March 2017, the Business Systems Team Leader advised that agreement with HR/Payroll had been made to obtain monthly payroll reports on 'starters, movers and leavers'. A process to follow up changes recorded with relevant managers to make necessary changes to network and SWIFT systems access will be undertaken to improve the management of change.

Strength of Internal Controls:	Moderate

Control Objective 3: To ensure that there are adequate controls for data input and data integrity in SWIFT

Audit Comments: Input:

Prior to inputting data in SWIFT, users are required to search records first to reduce the risk of data being input twice. Within the system there are warnings about creating new people where similar records may already exist. User guidance provides detail on search options to do this. Users are advised to search at a high level and use the 'wild card' option to provide numerous rows for checking. These rows of records are then to be refined filtered and sorted to verify if a record already exists. If none is found then a new record is created.

However, there is a risk that if the search option does not identify a record that is there, another record or duplicate may then be created.

Integrity:

Controls in place to assist with data integrity are reported as follows:

If a practitioner finds an error, such as a duplicate record, this can be reviewed and fixed through the formal request form for a record merging/deletion processed by the SWIFT Team. During January and February 2017 there were 1,240 new records created. 37 requests to merge records were made during that period, of which 15 were described as duplicate records or duplicate IDs. Record merge request forms are not kept by the system administrators; however, there is a record held within Swift about which records have been merged, who asked for it, when it was merged and who in the systems team merged it. This note is added into the actual client record to confirm the record that has been 'consumed' into the 'live' one. The email request is then deleted as the Team was advised that they should not keep records/data related to clients.

There are validation reports, some monthly; some related to a specific record/ assessment which can be run before a final version is saved

There are a number of guides on what information needs to be recorded, use of coded dropdown lists reduce input errors

In addition, the statutory social care return to the Scottish Government is an electronic extract of the SWIFT client details over the year. Considerable validation of this data is carried out prior to submission.

Other statistical analysis linking social care clients to NHS clients also assists with validating data and highlighting and duplicates.

Strength of Internal Controls:	Moderate

Control Objective 4: To ensure that there are adequate retention and output controls applied to SWIFT data

Audit Comments: Data Retention:

SWIFT data is kept electronically within the system and is not archived onto another storage area. This provides a single platform which makes search and retrieval of archives simpler and avoids compatibility requirements for a separate archive storage area.

No review was made on requests for data to be deleted as these records were not available during the review. In 27 September 2016, PKC employees were advised not to destroy any documents or files containing documents pertaining to children or interactions with children in the Inside News Bulletin.

Data Output:

Evidence of guidance for users on output controls was provided during the review. Council wide policy on safeguarding information beyond PKC, including the use of encryption and the use of USB hard drives confirmed policy guidance is in place for SWIFT users.

The Information Compliance manager reported that he understood the SWIFT system to be fairly well controlled. Evidence was provided of the PKC Data Protection Policy approved by PKC in February 2017. This defined roles and responsibilities for the security of personal and confidential data and data sharing agreement requirements. Further testing was not carried out as guidance and procedures were found to be in place for users to adhere to.

Audit trail and audit logs:

SWIFT audit logs have been switched on and report on data in the system going back to 2011. Systems administrators access and review these logs for incident management purposes and report on specific sensitive records data in SWIFT to relevant staff, but not for general compliance monitoring purposes.

Strength of Internal Controls:	Moderate

Management Action and Follow-Up

Responsibility for the maintenance of adequate and effective internal controls rests with management.

Where the audit has identified areas where a response by management is required, these are listed in Appendix 1, along with an indication of the importance of each 'action point'. Appendix 2 describes these action points in more detail, and records the action plan that has been developed by management in response to each point.

It is management's responsibility to ensure that the action plan presented in this report is achievable and appropriate to the circumstances. Where a decision is taken not to act in response to this report, it is the responsibility of management to assess and accept the risks arising from non-implementation.

Achievement of the action plan is monitored through Internal Audit's 'follow up' arrangements.

Management should ensure that the relevant risk profiles are reviewed and updated where necessary to take account of the contents of Internal Audit reports. The completeness of risk profiles will be examined as part of Internal Audit's normal planned work.

Acknowledgements

Internal Audit acknowledges with thanks the co-operation of the Business Systems Team Leader and Corporate IT during this audit.

Feedback

Internal Audit welcomes feedback from management, in connection with this audit or with the Internal Audit service in general.

Distribution

The final report will be issued to:

B Malone, Chief Executive

J Fyffe, Senior Depute Chief Executive

J Valentine, Depute Chief Executive

B Atkinson, Director of Housing and Community Safety

S Devlin, Director (Education & Children's Services)

A Taylor, Head of Corporate Revenues and IT; Housing and Community Safety

D Fraser, Head of Adult Social Work and Social Care

J Symon, Head of Finance

K McNamara, Head of Strategic Commissioning and Organisational Development

L Simpson, Head of Legal and Governance Services

G. Taylor, Head of Democratic Services

S Strathearn, Business Improvement Manager, Housing & Community Safety

D Henderson, Information Compliance Manager

C MacLean, Business Systems Team Leader

D Turner, (IT Co-ordinator (Applications)

External Audit

Authorisation

The auditor for this assignment was N Duncan. The supervising auditor was J Clark.

This report is authorised for issue:

Jacqueline Clark
Chief Internal Auditor
Date: 31 March 2017

Appendix 1: Summary of Action Points

No.	Action Point	Risk/Importance
1	End of Support Notice and security	Medium
2	SWIFT environments	Medium
3	SWIFT access and password authentication	High
4	User access management and change	Medium
5	Input and integrity checks	Medium
6	SWIFT record deletion	Medium

Appendix 2: Action Plan

Action Point 1 - System end of support notice and security

a) Although PKC has a contract agreement until the end of March 2019 with the supplier, Northgate has advised that a formal statement will be issued in April 2017 of the company's plan to end the development and support of SWIFT.

The Business Systems Team Leader chairs the Scottish SWIFT End User Group and this group has asked the supplier to consider extending support up to 5 years.

b) The Technical Support team is currently testing a security update to SWIFT for compliance with a target date for this upgrade in 31 March 2017. Therefore the risk arising from this vulnerability is limited to the testing period.

It is noted that dependence on third party suppliers' applications and older versions of system software is a general area of risk which is noted in the cyber security report to the Strategic Policy and Resources Committee in February 2016.

Management Action Plan

a) Once formal de-support notice is received, the Service will:

(i) Review the implications with Legal & Governance Services;

(ii) Carry out options appraisal for replacement system; and

(iii) Work with procurement, IT, system users to take forward tender process for replacement system.

b) The Service is working with the supplier (Northgate) and Corporate IT to ensure all relevant service packs are tested and applied as soon as possible after release.

Importance:	Medium
Responsible Officer:	S Strathearn, Business Improvement Service Manager/C MacLean, Business Systems Team Leader
Lead Service:	Housing & Community Safety
Date for Completion (Month / Year):	a) March 2020 b) complete
Required Evidence of Completion:	a) Replacement Social Care System Outline Business Case Tender/procurement documentation b) PSN Sign-off reports

Auditor's Comments

Satisfactory

Action Point 2 - SWIFT environments

Users learn SWIFT processes in the LIVE environment under supervision as there is no separate training environment. The risks of using the LIVE environment for user training include potential unauthorised change or loss of data.

Where there is a lack of segregation of duties available, mitigating controls can assist, for example review of audit trails and exception reporting.

SWIFT audit logs have been switched on and can report on system processes in reasonable detail back to 2011. Systems administrators have access to the audit logs and reporting function. Some audit reporting is carried out for specific sensitive records data in SWIFT.

Logs are reviewed on an incident response basis. There is no periodic random checking of the audit logs carried out.

Review of audit detail is a useful mitigating control, for example, to monitor areas where there is limited segregation of access, as referred to in action point 2 - users are trained in the live system and systems administrators can also input access.

Management Action Plan

The Business Systems Team Leader, in association with other relevant Team Leaders, will carry out periodic random checking of audit reports to confirm appropriate record access.

Importance:	Medium
Responsible Officer:	C MacLean, Business Systems Team Leader
Lead Service:	Housing & Community Safety
Date for Completion (Month / Year):	September 2017 and then 6-monthly.
Required Evidence of Completion:	Exception report from review of audit logs

Auditor’s Comments

Satisfactory

Action Point 3 - Access to SWIFT and password authentication

SWIFT users' first time passwords are issued to users via email on user request forms which are printed off and then countersigned, stored and can be viewed by others. This does not comply with the Information Security Standards or SWIFT's Confidentiality and Passwords, Looking after Information – Staff Awareness guidance which requires usernames and passwords to be kept confidential and not shared.

In addition, there is no enforced change of SWIFT user login passwords although this functionality is available. It was reported that when this had been switched on previously there had been problems, so the facility was left switched off. However, this hasn't been tested in the latest version of SWIFT. SWIFT users are advised to manually change their passwords on a regular basis.

Mitigating controls to compensate for this control not being enforced include the initial network login controls which enforce a change every 40 days.

Management Action Plan

The process for issuing passwords will be changed to ensure these are confidential to the user and the Acceptance Form will be updated accordingly.

Importance:	High
Responsible Officer:	C MacLean, Business Systems Team Leader
Lead Service:	Housing & Community Safety
Date for Completion (Month / Year):	April 2017
Required Evidence of Completion:	Documented Process for issuing passwords Updated Acceptance Form

Auditor's Comments

Satisfactory

Action Point 4 - User access management and change

The process for identifying changes to user access requirements has been reliant on managers acting on reports generated from Swift and notifying the Business Systems Team of such changes. This can lead to delays in ensuring that system access is restricted to only those officers who require those levels of access.

Management Action Plan

In addition to distributing reports generated from SWIFT, the Service will use HR/Payroll monthly reports on starters and leavers to identify changes to SWIFT users' job roles and will follow up access changes.

A process to follow up changes and make necessary changes to network and SWIFT systems access is planned.

Importance:	Medium
Responsible Officer:	C MacLean, Business Systems Team Leader
Lead Service:	Housing & Community Safety
Date for Completion (Month / Year):	May 2017 - ongoing
Required Evidence of Completion:	Monthly cross- checked (before and after) system access reports

Auditor's Comments

Satisfactory

Action Point 5 - Input and integrity checks

Prior to inputting a new record, users are advised on how to search in SWIFT in case there is a record for that person already in the system. Guidance recommends users search at a high level and use the wild card option to provide numerous rows for checking. These rows of records are then to be refined filtered and sorted to verify if a record already exists. If none is found then a new record can be created. However, there is a risk that if the search option does not identify a record that is there, another record or duplicate may then be created.

The extent of this risk occurring was found in the report maintained by the Business Systems Team and provided during the audit. During January and February 2017 there were 1,240 new records created. 37 requests to merge records were made during that period, of which 15 were described as duplicate records or duplicate IDs.

A process for identifying and correcting errors and duplicate records in SWIFT was reported as follows. When a user finds an error, such as a duplicate record, correction of the SWIFT record is through the formal request form for a duplicate record merging processed by the SWIFT Team. The Team keep a summarised record of the change on a spreadsheet, and then send back the form to the user who requested the change. The email request is then deleted as the Team was advised that they should not keep records/data related to clients.

Other integrity checking of SWIFT input data is in place, including validation reports and close scrutiny of records annually for the Scottish Government’s statutory social care return. Other statistical analysis linking social care clients to NHS clients assists with validating data and highlighting and duplicates.

Management Action Plan

The Service will continue to monitor data quality using reports distributed to team leaders and other relevant staff to review and action as required in preparation for data migration to the replacement system.

Importance:	Medium
Responsible Officer:	C MacLean, Business Systems Team Leader
Lead Service:	Housing & Community Safety
Date for Completion (Month / Year):	Ongoing
Required Evidence of Completion:	Copies of reports showing reduced errors

Auditor’s Comments

Satisfactory

Action Point 6 - SWIFT record deletion:

A SWIFT Record Deletion Request Form was provided during the review which was required to be approved by a Team Leader or Senior. Records that could be deleted with this process included - Whole Client Record; Profile Note; Contact; Referral; Assessment; Relation; Involvement; Review; Criminal Justice Service Report; Criminal Justice Service Order; Other.

Internal Audit did not review details of requests for data to be deleted as these records were not available centrally. However, there appears to be a potential risk that if a whole client record had been deleted in error pre- June 2016, the only log detail of this would be in the file of a key worker who requested this.

Management Action Plan

A process will be put in place to maintain records of deletions from SWIFT (subject to compliance with the current embargo on client record deletions associated with children).

Importance:	Medium
Responsible Officer:	C MacLean, Business Systems Team Leader
Lead Service:	Housing & Community Safety
Date for Completion (Month / Year):	May 2017
Required Evidence of Completion:	Record of deletions from Swift

Auditor’s Comments

Satisfactory