Perth and Kinross Council

Internal Audit Report

Integra Interfaces

March 2014

Scott-Moncrieff
business advisers and accountants

Perth and Kinross Council

Internal Audit Report

Integra Interfaces

Introduction

In March 2014 we reviewed the controls around the Integra finance system interfaces. Our review focused on two significant interfaces with the general ledger, specifically the residential care payments files produced by the Swift system and the payroll payments files produced by the ResourceLink system.

Background

The Council uses Integra as its main finance system, which comprises of a number of modules including purchase ledger, sales ledger and general ledger. This is the main source for financial reporting within the Council.

There are a number of other systems throughout the Council through which financial information is recorded. These include systems such as ResourceLink (Payroll), SWIFT (social work foster care and residential care payments) and PECOS (eProcurement).

All of the systems interface with Integra to ensure that all income and expenditure is recorded in a central source.

It is essential that there are effective controls over system interfaces to maintain the integrity and accuracy of data.

Scope

The review assessed the adequacy of the control environment for interfaces with the Integra system. This included system access controls at application and database level, data validation and monitoring as well as control over design of new/existing interfaces.

The feeder systems considered within the scope of this audit were SWIFT and ResourceLink.

The control objectives for this audit, along with our assessment of the controls in place to meet each objective, are set out in the Summary of Findings.

Acknowledgements

We would like to thank all staff consulted during this review for their assistance and co-operation.

Summary of findings

The table below summarises our assessment of the adequacy and effectiveness of the controls in place to meet each of the objectives agreed for this audit. Further details, along with any improvement actions, are set out in the Management Action Plan.

No	Control Objective	Control objective assessment	Action plan ratings				
			5	4	3	2	1
1	There are effective controls within Integra and sample feeder systems for the creation and import of interface files.	YELLOW				2	
2	Access at database level for in-scope applications is adequate to prevent manipulation of data	RED		1			
3	There are effective controls in place to ensure secure data transmission and storage of interface files.	RED		1	1	1	
4	There are appropriate controls in place to ensure that there is adequate validation of data input to Integra	YELLOW					1
5	There are effective monitoring controls in place to confirm the success or failure of interfaces	YELLOW				1	
6	There are effective controls over creation of or changes to interfaces with Integra	GREEN					
7	All changes to interfaces are subject to appropriate testing before becoming operational	GREEN					

Assessment	Definition
BLACK	Fundamental absence or failure of key control procedures - immediate action required.
RED	The control procedures in place are not effective - inadequate management of key risks.
YELLOW	No major weaknesses in control but scope for improvement.
GREEN	Adequate and effective controls which are operating satisfactorily.

Conclusion

Our review has identified that there is scope for improvement in the controls over Integra interfaces. Our audit did identify some areas of good practice in relation to the process for upload of files as well as the review of rejected items/taking corrective actions. We also noted that there were formal control processes in place for changes to applications.

The main areas where improvements are required relate to the creation and transmission of files and assurance over access controls at database level. The current processes and security measures in place for the creation and transmission of files do not provide assurance in relation to the integrity of the data being imported to Integra. In addition, there is a need to improve the controls in place over direct access to SQL and Oracle databases. We noted that, in the main, shared generic or default accounts are used by IT and respective suppliers to undertake database administration for Oracle databases of the in-scope applications. This means that it is not possible to attribute access and actions to a named individual. For SQL databases, we noted that direct access is provided to all domain administrators. This includes the Desktop team and there did not appear to be a clear business case for them to have such access. In addition, auditing is not sufficiently well configured to ensure that all access and actions are recorded.

We have provided a summary of the most significant issues arising from our audit in the Main Findings section below.

Main Findings

- There is a need to ensure development and maintenance of detailed procedural documentation as it relates to the creation, transmission and import of interface data files. This should provide step-by-step guidance on each of the key processes.

- Improved controls are required over direct, powerful access to Oracle and SQL databases as well as the auditing and monitoring of access. We noted that shared generic and default accounts were in active use meaning that it is not possible to attribute access to a named individual.

- A number of issues were identified in relation to the storage and transmission of interface data files. Files are not secured or encrypted at any point from their creation to import. Files are not stored securely and could be amended as they are saved in network folders in clear text format. In addition, files are not always transmitted in a secure manner with email being used in some cases.

Further details of the points noted above, as well as a number of less significant issues are included in the Management Action Plan.

Management Action Plan

In order to provide information regarding the priority/seriousness of our report findings, a ranking of the findings has been provided. The rankings are as follows:

Priority rating	Definition
5	Very high risk exposure – Major concerns requiring immediate Management attention.
4	High risk exposure - Absence / failure of significant key controls.
3	Moderate risk exposure - Not all key control procedures are working effectively.
2	Limited risk exposure - Minor control procedures are not in place / not working effectively.
1	Efficiency / housekeeping point.

1. Control objective: There are effective controls within Integra and sample feeder systems for the creation and import of interface files

Observation and Risk	Recommendation	Management Response
1.1 Interface Process Documentation We were provided with copies of the Finance Systems Team process notes that have been produced to define the interface management processes for both ResourceLink (payroll) and Swift (residential care) file transfers. During a walkthrough of the processes it was noted that some steps had been omitted from the documentation or were unclear. Further it was noted that some processes had not been documented (e.g. validation process) and, as a result, there was reliance on staff working knowledge. There is a risk that, by not maintaining detailed procedures for key system tasks, data may not be imported to Integra accurately or in a timely manner to support management reporting.	We recommend that management ensure existing procedures are updated to ensure the guidance is complete and accurate. These procedures should include the following: • Document control and ownership • Purpose and direction of all interfaces • Security and key controls • Validation and integrity checks • File definitions/build standards/process dependencies • Error handling • Contingency arrangements • Completion of control sheets • Key contacts	Management have updated the guidelines for all interfaces from the point that they are received by the Financial Systems Team. Records for the last 6 years were reviewed and revealed that there had been no incidents and that every data import over that period was both accurate and within the stated timescales. An annual review of all Financial Systems Guidelines will take place to ensure that, where changes have not been documented at the time of the change, they will be identified and documented through this review process. **To be actioned by:** A Craig, Senior Systems Development Officer **No later than:** May 2014 - Completed
		Priority **2**

Observation and Risk	Recommendation	Management Response
1.2 Access controls It is essential that effective controls are in place for the creation of files within the feeder application and within Integra for the import of files. We noted during our audit that there were two accounts active within Integra that could be used for importing files despite them no longer being required. It is recognised that these were disabled during the course of the audit and that network access would also have been required to use them. There is a risk that the passwords for these accounts continue to be used without the knowledge of the Finance Systems Team. This could result in files being imported without permission and the integrity of data within Integra being compromised.	We recommend management ensure that there is regular review of privileged/powerful Integra user accounts to gain assurance that only valid users have access to commands of a more powerful nature. These reviews should be performed at least every six months.	Management assessed that there was no risk that the accounts identified could be used to access Integra, as access requires Active Directory accounts and none existed. The current annual review of front facing Integra users will now include users with direct database access. Management assess that it is immaterial if the passwords were known, as the accounts could not be accessed. **To be actioned by:** A Craig, Senior Systems Development Officer **No later than: Completed**
		Priority **2**

2. Key control objective: Access at database level for in-scope applications is adequate to prevent manipulation of data.

Observation and Risk	Recommendation	Management Response
2.1 Database Access When users have direct access to the database they can amend data whilst avoiding the same level of controls that exist if they were using the application. First line database administration (DBA) is provided by the Council's IT team. The respective supplier is responsible for resolving any issues that are not resolved internally. For the three in-scope applications support is as follows (database in brackets): • ResourceLink – Northgate (SQL) • Swift – Northgate (Oracle) • Integra – Capita IBSolutions (Oracle). **Oracle database** Both the Council IT team and respective suppliers share access to accounts which allow powerful access to the database. One example is the sys account, the most powerful account in the Oracle environment. We noted that there is no monitoring of access or activity of these accounts. We also noted that auditing was not enabled at the database level. (Continued over)	1. We recommend management ensure that controls over database accounts are improved for both SQL and Oracle databases. All users should be provided with individual accounts to allow all access to be attributed to users. 2. Controls over default or generic accounts should be improved so that access to the password for such accounts is restricted. Consideration should be given to the implementation of an 'emergency break-glass' procedure whereby access to the passwords for such accounts is directly linked to a support request. On completion of the support request, the password should be reset by the trusted person responsible for the account. (Continued over)	1. IT will undertake a review of accounts with access to SQL and Oracle with a view to implementing individual accounts for each user who has an operational need to access the database. 2. Default and generic accounts will be restricted to named individuals within PKC who will then grant access to members of staff who require access to these accounts. The named individuals will then reset the passwords once the task has been completed.
		Priority **4**

Observation and Risk	Recommendation	Management Response
2.1 Database Access cont. **SQL database** From review of active accounts for the ResourceLink SQL we noted that all IT staff in the Active Directory domain administrators group have direct, powerful access to the SQL database. This includes the server team and desktop team. There may be a business need for the server team to have access to perform work on the SQL server however, there appears little justification for the desktop team having such access. We also noted that two accounts belonging to development staff were active in the SQL server. One of these was said to be a temporary account. Furthermore, auditing at the database level is limited with only failed logins being recorded. It was stated that the sa account, a default account and the most powerful in the SQL environment, was not actively used and a copy of the password is maintained in a safe. There is no monitoring of the use of the sa account or general activity in the SQL environment. There is a risk that access made at the database level cannot be attributed to a named user. There is also a risk that data within the database could be changed to perpetrate a fraud and this would not be detected and the responsible party identified.	3. We recommend that audit functionality within both Oracle and SQL databases is activated to ensure that all relevant user activities are recorded. The log files should be stream to a syslog to reduce the risk of the log files being amended by a user with powerful access. We also recommend that there is regular monitoring of log files to gain assurance that all access is appropriate. 4. We also recommend that access controls for the ResourceLink database are improved. This should ensure that only valid IT officers with the skills and knowledge of database administration are provided with access. In particular, access for development staff to the live environment should be disabled as a matter of course, with access only being granted in response to a service request/incident. This access should also be subject to monitoring.	3. Audit logging on systems is often not recommended by suppliers as it can cause performance issues with the system. IT will liaise with business system owners and suppliers with the view to activating logging. Residual performance issues – should they arise - will be investigated. 4. See 1 and 2 above. **To be actioned by**: E Walker, Team Leader, Information and Applications Management **No later than:** December 2014

3. Control objective: There are effective controls in place to ensure secure data transmission and storage of interface files

Observation and Risk	Recommendation	Management Response
3.1 Secure Storage of Files A number of interface files are transmitted by email and are also stored on local network drives at both the source and recipient. These include: a. Supplier payments for residential care b. Payments to individuals for child fostering Similarly some other data files are collected from source systems and these are also stored on local network drives. During the time the files are stored on local network drives, they are not encrypted or password protection. They are only protected by standard network security meaning that anyone who has access to these network areas would be able to read, change, copy and delete data in the files. It is recognised that there are controls in place at later stages in the process (e.g. reconciliations, review of exception reports) which provide an additional level of control. (Continued over)	1. We recommend that IT is requested to provide lists to relevant line managers which detail those users with access to network folders that are used to store interface files. These should be reviewed by line managers to confirm that only those involved in the interface creation, transmission and import have access to the files. Where amendments are required these should be notified to IT to ensure access is revised. This exercise should be conducted on a regular basis. 2. We also recommend management ensure that consideration is given to providing additional security to stored files to protect the data from loss and change. File encryption may be considered as an option to address this issue. We also recommend that automated solutions for file transfers are investigated. This should aim to eliminate the current process of clear text files being transmitted in unencrypted format across the corporate network. This should seek to ensure that files are encrypted at all stages of the process.	1. There has been a review of permission levels for local network drives containing interface files and Services are content that these are now appropriate and will be maintained through the routine verification processes. IT will provide a list of users with access on a regular basis. Any changes to access required will be logged through IT and authorised. 2. The Information Compliance Manager has stated that good control over network access and checks on the created date / last modified date should achieve the same result as encryption as the files are not transferred outside the Council network. It should be noted that these files do not contain any supplier name only coded supplier references. (Continued over)
		Priority **3**

Observation and Risk	Recommendation	Management Response
3.1 Secure Storage of Files cont. We examined the user access list for the network location where payroll files are stored, both at point of creation and for import. We noted that, in addition to the Finance Systems Team, there were 5 further user accounts with access to this area. These related to 4 IT staff and 1 external consultant. It was confirmed that these user accounts were now redundant, with one never having been valid in the first place. The accounts belonging to specific individuals within IT were notified to management at the time of the audit and the access rescinded. We also noted that there was a test account live in the 'T drive' (named Bev Test). There is a risk that the data files for interfaces are at risk of being edited or deleted. This could result in erroneous data being imported to Integra. If this was to happen, financial reports would be inaccurate and this could affect decision making.		**To be actioned by:** K Barron, IT Team Leader Business Applications **No later than:** August 2014

Observation and Risk	Recommendation	Management Response
3.2 Data Retention Periods Through our discussions and review of documentation, we identified that there is no formal retention period defined for interface data files. Staff are currently operating to a 6 years plus current basis. As a result, all files produced since the interface implementation are being stored (and backed up) on the network drives. We did note that the oldest file (relating to Swift interfaces) retained dated back to 2010. The lack of clear guidance on retention of interface data files could result in data being held for longer than is necessary.	We recommend that the requirements for retaining interface data files are determined. Once this is done, a formal policy should be developed and implemented to ensure that files are only retained for as long as necessary. There are likely to be two options for management: (a) The files are regarded as financial information and therefore should be retained for the same period as core financial information (typically current year + 6 full previous years); or (b) The files are one-off inputs and can be deleted after use due to the fact that the data will be in both the feeder system and Integra.	The Service will determine the business need for retaining this information and ensure that this is clearly articulated. **To be actioned by:** C Barnett, Finance Officer, Housing & Community Care **No later than:** September 2014
		Priority **2**

Observation and Risk	Recommendation	Management Response
3.3 Data Transfer Requirements We noted from our discussions and review of data files that the Social Work supplier payments files are emailed from Social Work to the Finance Systems Team. At the same time, it is also emailed to both Social Work and the Social Work Budgeting Team. We noted that the one file includes cost information that is detailed by service user name. This results in personal data being transmitted and made available to personnel within the Council who have no need to see this. There did not appear to be any legitimate reason for providing such information to the Finance Systems Team. During discussions with staff it was agreed to separate the data and that only the data required by the Interface file would be sent in future. It was also indicated that the file would be stored in a different network folder which would be accessible to budget staff to avoid the need for emailing such information. By using email, there is a risk that the file is sent to the wrong recipient. This could result in a breach of the Data Protection Act and give rise to negative publicity.	We recommend management ensure that interface files contain the minimum required data and avoid including personal data unless unavoidable. In addition, in accordance with MAP3.1, alternative solutions are investigated for the transfer of files. We also recommend that budget staff do not have access to the source interface file.	Only the file required for the interface is emailed to Finance Systems Team. This change was undertaken with immediate effect once the issue had been raised. **To be actioned by:** C Barnett, Finance Officer, Housing & Community Care **No later than:** Completed
		Priority **4**

4. Key control objective: There are appropriate controls in place to ensure that there is adequate validation of data input to Integra.

Observation and Risk	Recommendation	Management Response
4.1 ResourceLink Data Validation The Information Systems and Development Team will run validation reports on the data prior to the creation of the files to be transferred. This report will highlight any instances of invalid or missing GL cost centre codes. Corrections are carried out and reports re-run but this is subject to time constraints. This is to ensure that staff are paid on time. When the transfer date is reached, the resolution of errors is stopped and the file is transferred to the Finance Systems Team for its import to Integra. Any further errors (mainly incorrect or missing GL cost codes) are then identified through the interface process. They will be returned to the Payroll Team/Accountants for fixing or creation of appropriate journals. Errors will usually be corrected within the following ledger period. We noted that there are occasions where payroll is processed without valid GL codes and it appears to be the accepted norm that these will be addressed as part of the interface process. (Continued over)	We recommend management undertake an exercise to identify the key factors that contribute to coding errors within the payroll system.	The Service state that the primary function of a payroll system is to allow the employer to comply with legislation, by paying employees accurately and on time. In 2013/14, there were 1,072,578 lines of G/L code interfaced from payroll (ResourceLink) to the ledger (Integra), in respect of the two main Council payrolls. Of those lines, 247 lines were interfaced with wrong or missing G/L codes. This represents an error rate of 0.02%. This very low error rate is as a result of a number of controls being in place prior to the payment deadline and the Council will not hold up the payroll until these remaining coding issues are dealt with. The primary controls are the requirement for employees to record the correct code, managers to check that the code is correct and the payroll team contacting Services to obtain clarification of codes where the cost code is not recorded on ResourceLink. These controls results in the correct codes being applied for 99.98% of transactions. (Continued over)
		Priority **1**

Observation and Risk	Recommendation	Management Response
4.1 ResourceLink Data Validation cont. This appears to be inefficient due to the retrospective nature of the work. Management is aware of this issue but there does not appear to have been any exercise conducted to establish how to reduce the volume of errors on a monthly basis. There is a risk that resources are not being used efficiently and effectively due to issues being resolved retrospectively. There is also a risk that financial reports may not be accurate.		The report acknowledges that there is a third G/L code verification control process undertaken post interface which allows for the correction of the monthly average of 21 errors (247 errors in 2013/14 divided by 12 months), but identifies a risk that the "Resources are not being used efficiently and effectively due to issues being resolved retrospectively." Management commend staff for their diligence and hard work in resolving the vast majority of code errors before the third process. Nonetheless, discussions with Services will be undertaken over the course of 2014 to explore what might be done to improve the accuracy of G/L coding in source documentation. **To be actioned by:** E Sturgeon, Chief Exchequer Officer **No later than:** December 2014

5. Key control objective: There are effective monitoring controls in place to confirm the success or failure of interfaces.

Observation and Risk	Recommendation	Management Response
5.1 Control Sheets The methods of recording the actions taken with the interface files in the Finance Systems Team vary according to the source of each file. It was noted that the ResourceLink (payroll) files are accompanied by a control sheet that details the name and value of the transferred files. This control sheet also requires that staff processing the file record their initials on the sheet for each stage of the process. The control sheet informs the process by providing a clear audit trail of who completed each stage of the upload process and confirms that task has been completed. While it is acknowledged that the interfaces have different requirements (processes vary according to the particular ledger being updated), this is not replicated across all interfaces. There is a risk that, without the control sheet, it may not always be clear what actions have been taken and by whom and that each week's processing was carried out.	We recommended, as good practice, that control sheets are introduced for all interfaces with Integra. Consideration should be given to modifying the current form used for Payroll but ensuring that this includes the names of files received and processed as well as control totals. Staff should also initial the form to confirm the various stages of the process have been completed.	Management have introduced control sheets for all interface files from July 2014 **To be actioned by:** A Craig, Senior Systems Development Officer **No later than:** July 2014 - Completed
		Priority 2

6. Key control objective: There are effective controls over creation of or changes to interfaces with Integra.

We have found no significant issues in relation to this control objective.

We noted that changes to the in-scope applications are limited to general updates received from the respective vendor. We noted that such updates have to follow a formal control process. We reviewed documentation which evidenced that changes were subject to formal review, risk and impact assessment and approval before being released to the live environment.

7. Key control objective: All changes to interfaces are subject to appropriate testing before becoming operational.

We have found no significant issues in relation to this control objective.

We identified that there is formal user acceptance testing performed where there is a change to the application. We also identified that, where relevant, the testing includes interfaces. We also noted that user acceptance testing is documented with each noted as having passed or failed.