Internal Audit Report
Corporate and Democratic Services
Review of Internal Controls
18-02
December 2018

Final Report
(Report No. 19/28)

Legal and Governance
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)

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 2018/19, which was presented to the Audit Committee on 27 June 2018. This review follows on from the earlier update to Audit Committee on 23 May 2018 by the Chief Internal Auditor (Report No. 18/168) on the first phase of work. In this phase, Internal Audit ascertained that relevant Council Services were aware of the contents of an Audit Scotland report that detailed a significant fraud at Dundee City Council (DCC). The Head of Finance, as the Section 95 Officer per the Local Government (Scotland) Act 1973, was aware of the content of the report and had taken action including the circulation of the findings to relevant officers within the Council; the Financial Systems Team Leader, the IT Service Manager and IT Team Leader were all aware of the report.

In this second phase of work, audit focused on the four fundamental controls highlighted by Audit Scotland and whether they were operating effectively. Audit testing was carried out in October and November 2018. Examination of controls in place included those in place to reduce the potential for internal and external threats to integrity of supplier payments.

Scope and Limitations

The audit focused on controls for processing supplier payments through feeder systems and reported in Integra Purchase Ledger. Controls must take into account the need for the Council to report on meeting targets for paying invoices promptly. The Council is required to provide a performance indicator on the number of invoices paid within 30 days of receipt (or otherwise agreed credit terms). An analysis of the Council’s payments profile found that 94% of invoices are up to £5,000 and 64% are under £250. In addition to the three weekly batches of creditors payments normally run, separate processing of urgent invoices is made through BankLine system. All invoices are subject to scrutiny as defined in the Council’s financial regulations.

Testing included interviews with key officers in Corporate & Democratic Services including the Financial Systems [FS] Team, and the IT Business Applications Team. A review of relevant procedures and documentation was also carried out.

Excluded from scope is detailed examination of payments made via procurement cards and Concerto.

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 the adequacy of segregation of duties controls and ensuring access to systems are restricted to appropriate levels (to negate the possibility of individuals processing transactions all the way through the payments process).
Internal Audit Comments: Segregation of duties was reviewed both within and across the following systems – Integra Purchase Ledger, PayGate software for processing BACS files, and BankLine for processing urgent payments. The DCC case involved sub-systems for paying suppliers - the Fleet Management system and an in-house Construction Industry Scheme [CIS]. Therefore these were also reviewed within the Financial Systems (FS) Team. It was found that although access to supplier bank account data was limited to a small number of FS Team administrators, the high level access within Integra gave administrators privileges to access all data fields, not just supplier bank detail therefore segregation of duties was not available as a single control for integra. Instead, controls included having no single officer with sole high level access. There are four system administrators in Integra, four system administrators in PayGate and two administrators for the BankLine system. In addition any changes to bank account data fields are reported in the integra audit logs. Furthermore reports run during the review confirmed that usernames logged as having changed supplier bank accounts in integra Live were all authorised to carry out this task. Two finance officers were found to have system administrator access across three systems - Integra, PayGate and BankLine. Privileges were used as the control to restrict their access; for example they were not allowed to input data in BankLine. Two IT database administrators also had access to Integra data tables to carry out maintenance of the live system and patch management. In practice, file naming protocols for data tables made the files difficult to identify and reduced any potential for unauthorised changes. The same two IT database administrators also had access to maintain PayGate software. However this ended during the audit as PayGate moved off Council servers onto the cloud under a new contract with the supplier. The Council's bank had recently reviewed 13 areas of security for BankLine and made 5 recommendations for increased security. Of these, 2 were changed; another two were reported to be for functions not used by the Council so not relevant; and the risk of 1 recommended area was tolerated as there were already compensatory controls in place through payments requiring to be dual authorised. Additional controls are applied to monitor larger value invoices against recent changes to bank accounts before they are paid. The FS Team are currently reviewing thresholds for monitoring supplier payments for improved security.

A new ‘e-form’ is being designed and tested by the FS Team to manage requests for changes to suppliers’ details. The new form process is designed with layers of control checks – an initial check is completed by the service as per guidelines, then a second check will be completed in the Financial Systems team contacting the supplier before any changes are made to a supplier’s data. This new form is expected to go live early in 2019 and provides another level of control to payments to suppliers. Authorisation levels are maintained in the Finance Services Authorised Signatories Register. The Construction Industry Scheme [CIS] was reviewed and this was found to have adequate segregation of duties. The Fleet Management system does not interface to Integra in the Council so can be excluded from this review in terms of risk.	
Strength of Internal Controls:	Moderately strong

Control Objective 2: To ensure that feeder systems are effectively reconciled to other systems – specifically the Purchase Ledger; using third party information (supplier's statements) and reconciling with payment systems for payments of creditors.	
Internal Audit Comments: Reconciliations of the 6 feeder systems to Integra are all documented and updated by the FS Team. In practice, reports on successful batch runs for 3 of the 6 interfaces are not sent back to the Services unless there were any discrepancies in the interface runs. The 3 system interfaces which had not asked for notification of successful runs were reported to be Northgate Council Tax & Rates, SEEMIS clothing grants and SWIFT Residential Payments. Results from the other 3 interface batch runs were notified to the relevant Service area. Pecos orders are automatically interfaced for increased control. Payment of invoices can be made without a matching purchase order and third party statements are not used for reconciliation for all 6,000 active suppliers as this is too resource intensive. In both cases the authorisation process is the primary control. In the DCC incident, suspense accounts were reported to be used. The Corporate Accounting Manager advised that a sample of suspense account reconciliations is independently checked on a monthly basis. A check on old in-house developed systems found one in use that the IT Business Applications Team had no awareness of – Bank Reconciliation. This system was reported to be used regularly by the Finance Manager for reconciliations of cheques and income.	
Strength of Internal Controls:	Moderately Strong

Control Objective: To ensure that system documentation is maintained which details key controls to be carried out by staff to prevent fraud or error in payments of creditors.
Internal Audit Comments: Substantial documented procedures for Integra Purchase Ledger and interfaces with sub-systems were provided on request by the F S Team during the review. In addition to the Purchase Ledger User Manual on Eric for system users, there were procedures for system administrators managing batch processes for all interfaces to Integra Purchase Ledger. Procedures for daily processes and daily control reporting for balance checks and corrections for the transaction consolidation in the Purchase Ledger were documented. For interfaces to Purchase Ledger, there were separate procedure notes for – • Concerto to Integra to Concerto v2 • Clothing grants • EMA Interface Instructions • SWIFT Interface Instructions • Council Tax and Rates • Foster Carer interface instructions • Purchase Card interface • Guidance for the Daily PECOS Interface to Integra There were also procedures on Construction Industry Scheme and payments to suppliers or sub-contractors.

Strength of Internal Controls:	Strong

Control Objective: To ensure that budget monitoring is at a level that allows budget holders to identify anomalous payments to suppliers at an early stage.
Internal Audit Comments: It was reported that monitoring revenue expenditure carried out was unlikely to identify the value of transactions that were involved in the DCC fraud case. The fraud carried out at DCC was carried out using a large number of small value transactions in service areas where variances were expected to occur. It is noted that the Council has controls in place for higher value transactions of £50k and £75k. Whilst the Audit Scotland report on the DCC case recommended that budget monitoring should be at a level that would allow budget holders to identify anomalous payments at an early stage, the payment profile for the Council shows the majority of supplier payments are under £5000 and there are very many of these. Therefore the Council's controls for identifying anomalous payments lie elsewhere in the payment process, for example controls found in the first objective above. During the audit there was consideration underway of the use of new pre-emptive

monitoring of invoices prior to their payment. Although this was mainly to identify potential duplicates, it might also assist in identifying other anomalous invoices in advance of payment. The Council's insurance cover in the event of fraud occurring has a £5,000 excess on each claim.	
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 Finance System Team and the IT Business Applications Team during this audit.

Feedback

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

Distribution

This report has been distributed to:

K Reid, Chief Executive

J Valentine, Depute Chief Executive (Chief Operating Officer)

L Simpson, Head of Legal and Governance Services

S Mackenzie, Head of Finance

A Taylor, Head of Corporate IT and Revenues

S Walker, Chief Accountant

J Cockburn, Finance & Governance Manager

C Robertson, Central Services Manager

F Crofts, Finance & Resources Manager

A O'Brien, Corporate Services Manager

L Law, Financial Systems Team Leader

D Adams, IT Service Manager

D Turner, IT Team Leader (Business Applications)

Committee Services

External Audit

Authorisation

The auditor for this assignment was N Duncan. The supervising auditor was M Morrison.

This report is authorised for issue:

_____

Jacqueline Clark
Chief Internal Auditor
Date: 19 December 2018

Appendix 1: Summary of Action Points

No.	Action Point	Risk/Importance
1	System Administration duties and privileged access	Medium
2	Supplier amendment e-form	Medium
3	Interfaces and batch runs	Low
4	In-house legacy application and IT support	Medium
5	Monitoring larger payments and changes to bank accounts	High

Appendix 2: Action Plan

Action Point 1 - System Administration duties and privileged access

System administrators within the FS Team require and have high level access to carry out their work. Integra high level access allows users with system administrator privileges to change standing data including supplier bank account data. These changes are reported in the audit tables of the financial management information system.

As there is a small FS Team, some officers have system administrators' access across more than one system that invoices are processed through. Integra logs changes to bank account data fields.

Controls in place for separation of duties include not only audit logs but also dual access; no one single administrator has high level access.

Reports run during the review confirmed that usernames logged as having changed supplier bank accounts in integra Live were all authorised to carry out this task.

As a result of the high level access it may be possible to process a transaction through the payments process and although this would be highlighted in the logs there is benefit in introducing an additional control check.

Management Action Plan

An alert will be created where changes to supplier details are processed by unauthorised officers and this will be sent to Central Services Manager and the Financial Systems Team Leader in real time.

Risk/Importance:	Medium
Responsible Officer:	L Law, Financial Systems Team Leader
Lead Service:	Corporate & Democratic Services
Date for Completion (Month / Year):	January 2019
Required Evidence of Completion:	Evidence of report generation

Auditor's Comments

Satisfactory

Action Point 2 - Supplier Amendment ‘e-form’

The new supplier amendment e-form is currently being designed and therefore yet to be tested. This new form is expected to go live early in 2019 and provides more control checks to payments to suppliers.

Management Action Plan

Once the new e-form has gone live in 2019 and sufficient data is available, the FS Team will review the form and processes to confirm it is reducing manual processes and improving security.

Risk/Importance:	Medium
Responsible Officer:	L Law, Financial Systems Team Leader
Lead Service:	Corporate & Democratic Services
Date for Completion (Month / Year):	March 2019
Required Evidence of Completion:	Outcome from the review

Auditor’s Comments

Satisfactory

Action Point 3 - Interfaces and positive assurance of batch runs

Of the six interfaces to Integra Purchase Ledger, three interfaces report back to Services that batch input has been run successfully with no errors. The other three interfaces (for Northgate, SWIFT & SEEMiS (clothing grants)) do not get reports back to Services from the FS Team that batch input has been successful as they have not requested this positive assurance.

IT processing good practice includes providing validation reports and positive assurance that batch processing has been successful.

Risks of not providing this positive assurance include potential lack of evidence to confirm batches are successful.

Management Action Plan

The Service will contact the three Services who do not get reports back to be advised that they will receive positive assurance that batches have run successfully in future runs.

Risk/Importance:	Low
Responsible Officer:	L Law, Finance Systems Team Leader
Lead Service:	Corporate & Democratic Services
Date for Completion (Month / Year):	February 2019
Required Evidence of Completion:	Reports provided to the three Services

Auditor's Comments

Satisfactory

Action Point 4 - In-house legacy application and IT support

A review of Council IT developed in-house applications found a system called Bank Reconciliation, developed many years ago and still used on a regular basis by the Central Services Manager for day to day work. IT Business Applications Team officers were not aware of the use of this application, as support for this was provided by a software engineer in the IT Transformation Team. Procedure notes were not available and an IT engineer reported it may not be compatible with the planned rollout of Windows 10.

It would be an operational loss if this system support was not available until an alternative product was sourced. Also there may be a risk that other old systems not compatible with Windows 10 are still used by Finance officers. There is benefit in undertaking a review of all applications to ensure they are supported and documented.

Management Action Plan

The IT Teams will review the old in house application for Bank Reconciliation that has no documented procedures and may be at risk with rollout of Windows 10.

Any other legacy applications will be reviewed for continued support by Business Applications IT Team.

Risk/Importance:	Medium
Responsible Officer:	D Turner, IT Team Leader (Business Applications)
Lead Service:	Corporate & Democratic Services
Date for Completion (Month / Year):	
Required Evidence of Completion:	Outcome from review

Auditor's Comments

Satisfactory

Action Point 5: Monitoring larger payments and changes to bank accounts

Supplier payments at /above the value of £50,000 are specifically reported and reviewed against the date of latest bank account change for that supplier. This control is checked before any payment is made. As there are an increasing number of supplier payment frauds being attempted, local authorities are alerted to risks and the Council's bank has provided guidance to Finance officers in this regard. There is no commensurate control to ensure that payments below this threshold are monitored to the same degree. Following a review of the Council's payments which found that 94% of payments were less than £5,000 the FS Team are reviewing the threshold level for monitoring payments against changes to bank accounts.

Management Action Plan

The FS Team review of the threshold level for monitoring payments against changes to bank accounts will take into account the increasing number of supplier payment frauds being attempted.

Risk/Importance:	High
Responsible Officer:	L Law, Finance Systems Team Leader
Lead Service:	Corporate & Democratic Services
Date for Completion (Month / Year):	March 2019
Required Evidence of Completion:	Outcome of review

Auditor's Comments

Satisfactory