Internal Audit Report
Corporate and Democratic Services – Finance Division
IT Application review - Optimum No. 15-35
March 2016

Final Report

Chief Executive’s Service
Finance Division
Perth & Kinross Council
2 High Street
Perth PH1 5PH

Internal Audit

Background and Introduction

This assignment forms part of the Internal Audit plan for 2015/16 and was approved by the Audit Committee on 1 April 2015.

The Optimum time recording system is used across the Council to record hours worked by staff and has been in place for a number of years. The system links with the Resourcelink HR/Payroll system. Both systems are provided and supported by NorthgateArinso.

Scope and Limitations

In order to arrive at an opinion on the achievement of the control objectives, the audit included interviews with relevant staff in Information Technology and Finance Division within Corporate and Democratic Services.

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. There are adequate system administration and user procedures.	
Auditor's Comments: It was demonstrated that an e-learning module for the Optimum system was available to all staff (with a PC) at their induction. This is accessible to all other staff as a refresh tool. Both the Optimum end-user and system administration guidance documents were noted as being up to date for the current version of the software.	
Strength of Internal Controls:	Strong

Control Objective: 2. There are robust logical access controls	
Auditor's Comments: Optimum users are required to have a username and password. Most users login through 'My view' via the Single Sign-On process. The Optimum system minimum password requirements are 8 characters (comprising of upper and lower case alpha and numeric characters). The system also prompts users to change their passwords every 42 days. We also noted that all user accounts are locked after 3 successive failed login attempts.	
Strength of Internal Controls:	Strong

Control Objective: 3. There is effective user account management which ensures only authorised users have access.

Auditor’s Comments: It was demonstrated that an individual’s access is authorised by their line manager. The access provided is the minimum access required for users to input their work hours within Optimum. There is also an authorised signatory list for line managers and system administrators and this is recertified on an annual basis. New start accounts are set up in response to receipt of Employee Services and line managers’ approvals.

Leavers’ accounts are disabled at the relevant leaving date. This process is based on an established interface with Resourcelink which generates an email to the appropriate Optimum administration team.

No exceptions were noted from our testing.

Strength of Internal Controls:	Strong

Control Objective: 4. User access levels are appropriate and ensure adequate segregation of duties in relation to the administration and operation of the system.

Auditor’s Comments: Segregation of duties is enforced through the use of access profiles. The system security design also ensures that line managers and administrators cannot modify their own timesheets.

Staff can input time and make corrective adjustments which then require line-manager approval. There is also a verification exercise carried out by the Information Systems Development (ISD) team which confirms Operator (i.e. line manager) and Administrator access is valid and appropriate.

Strength of Internal Controls:	Strong

Control Objective: 5. Access to amend system parameters is restricted to authorised users.

Auditor’s Comments: We confirmed that system parameters are only accessible to system administration staff. This access allows them to set up and assign work patterns, rosters and contracted hours. These match the employee information set up in Resourcelink. These parameters also determine the appropriate trigger points for errors and exceptions. For example, these are used to alert staff where clock in/out times are missing and for end of period reports on user time balances.

We noted that there were 791 work rosters, 127 types of contracted hours and 244 work patterns setup within the Optimum system. We also noted that not all rosters had Council staff assigned to them.

We were informed that there is no housekeeping carried out on this standing system data to ensure that only relevant rosters, contracted hours and work patterns are maintained within the system. By not ensuring that only valid standing system data is maintained, there is a risk of staff being assigned to an invalid or incorrect roster, work pattern or contracted hours profile. It is recognised that such errors would likely come to light when a user and/or their line manager reviews their timesheet. Whilst not presenting a significant risk, it results in a marginal reduction in the effectiveness and efficiency of administration of the Optimum system.

Strength of Internal Controls:	Moderate

Control Objective: 6. All data interfaces ensure complete and accurate transfer of data.

Auditor's Comments: It was observed that there were two interfaces with the Optimum system, both of which were from the Resourcelink HR and Payroll system. These are 1) to notify of the creation of a new start, and 2) the processing of a leaver. When data is transferred, the Optimum system will generate an email notification for the Optimum Worktime Leave and Supply (OWLS) team. The OWLS team confirms each change notification by reference to the Optimum system and any discrepancies are corrected manually.

Strength of Internal Controls:	Strong

Control Objective: 7. There are effective data input and validation controls.

Auditor's Comments: The data input parameters are determined by the work-pattern, roster and contracted hours assigned to each user. Any infringements of the core hours, etc. are alerted to the user (on their timesheets) and these are also visible to their line manager when reviewing their team's timesheets online. All managers are required to review their team's time records and approve adjustments that are made as well as follow-up on any outstanding time issues.

It is understood that this process operates effectively although this is based on an expectation that all managers are performing regular reviews (at least weekly) and challenging employees' adjustments as required.

Strength of Internal Controls:	Strong

Control Objective: 8. Adequate backup, recovery and continuity procedures are in place.

Auditor's Comments: Backups are performed daily. The Monday – Thursday backups are incremental (changes from the previous one) and a full back up is performed each Friday. Evidence demonstrated that the Symantec Netbackup system sends a report confirming if the back-up was successful or not. If unsuccessful, the IT team would re-run the backup and take any action required to further investigate and correct the issue. IT carries out regular restores of files and folders to provide assurance in relation to the backup and recovery process.

It was stated that, in the event of the Optimum system being unavailable, the clock-in systems would continue to operate and store the data (provided they had power available). Once Optimum has been restored data can then be synchronised and updated. The system is not regarded as a "critical" business system. As a result, there is no documented System Recovery Plan for Optimum and there has not been a planned system recovery test carried out. As the system is not regarded as critical its restoration in the event of a wider IT disaster is based on best endeavours. Whilst recognising there is some resilience in the form of the clock-in systems, it is not clear how long these would continue to retain data indefinitely in the event of a prolonged system outage.	
Strength of Internal Controls:	Moderately strong

Control Objective: 9. There are appropriate audit facilities within the system to allow effective and regular monitoring of the application.	
Auditor's Comments: It was stated that there were audit logs available should they be required. Currently log reports can be produced on a reactive basis following a request to NorthgateArinso. However, there is currently no proactive monitoring of access made by those users with the System Administrator role profile to confirm that it is appropriate. As noted above (Control Objective 7), the ISD team is currently working on a project with NorthgateArinso to develop additional reporting and it is anticipated that audit log reports will be created as part of this exercise.	
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 Information Technology and Finance Division staff from within Corporate and Democratic Services during this audit.

Feedback

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

Distribution

B Malone, Chief Executive;

J Walker, Depute Chief Executive for Corporate and Democratic Services

J Symon, Head of Finance, Corporate and Democratic Services

A Taylor, Head of Corporate IT and Revenues, Corporate and Democratic Services

E Sturgeon, Chief Exchequer Officer, Corporate and Democratic Services

S Liston, Team Leader, ISD

K Wilson, Corporate IT Manager

K McNamara. Head of Strategic Commissioning & Organisational Development

G Taylor, Head of Democratic Services

P Dickson, Complaints & Governance Officer

External Audit

Authorisation

The auditors for this assignment were A Munn (Scott-Moncrieff) and A Mauree (Scott-Moncrieff). The supervising auditor was P Kelly (Scott-Moncrieff).

This report is authorised for issue:

____

Jacqueline Clark
Chief Internal Auditor
Date: 4 March 2016

Appendix 1: Summary of Action Points

No.	Action Point	Risk/Importance
1	Review of standing data	Low
2	Disaster recovery and business continuity planning	Low
3	Production of audit logs	Low

Appendix 2: Action Plan

Action Point 1 - Review of Standing Data

Our review identified that there are currently 791 work rosters, 127 types of contracted hours and 244 work patterns set up within the Optimum system.

There has not been any review performed of standing system data such as work patterns, contracted hours and rosters to confirm their ongoing relevance. For example, we noted that there were rosters available within the system that had no staff assigned to them. This could result in errors being made in the assignation of rosters, work patters and contracted hours to staff resulting in additional work having to be performed to correct this.

Management Action Plan

The Service were aware of the complexities of the standing data with regard to work patterns. Once the final phase of the migration of Education & Children's Services staff onto Leave Management, there will be a housekeeping exercise undertaken to ensure that only those work patterns which are current are retained.

This will avoid the need to remove standing data which may be subsequently required in the final phase

Importance:	Low
Responsible Officer:	S Liston, Team Leader ISD
Lead Service:	Corporate & Democratic Services
Date for Completion (Month / Year):	February 2017
Required Evidence of Completion:	Email from Team Leader to Internal audit confirming housekeeping has been completed.

Auditor's Comments

Satisfactory

Action Point 2 - Disaster recovery and business continuity planning

It was stated that, in the event of the Optimum system being unavailable, the clock-in systems would continue to operate and store the data (provided they had power available). Once Optimum has been restored data can then be synchronised and updated.

The system is not regarded as a “critical” business system. As a result, there is no documented System Recovery Plan for Optimum and there has not been a planned system recovery test carried out. As the system is not regarded as critical its restoration in the event of a wider IT disaster is based on best endeavours.

Whilst recognising there is some resilience in the form of the clock-in systems, it is not clear how long these would continue to retain data indefinitely in the event of a prolonged system outage.

Management Action Plan

The Team Leader ISD will seek confirmation from NGA (NorthgateArinso), the supplier, on how long the clocks would continue to retain data indefinitely in the event of a prolonged system outage. Once known, this timescale will be assessed as to its usefulness in a recovery situation.

Importance:	Low
Responsible Officer:	S Liston, Team Leader ISD
Lead Service:	Corporate and Democratic Services
Date for Completion (Month / Year):	June 2016
Required Evidence of Completion:	Email from NGA

Auditor’s Comments

Satisfactory

Action Point 3 – Production of audit logs

It was stated that there were audit logs available should they be required. Currently log reports will be produced on a reactive basis following a request to NorthgateArinso. However, there is currently no proactive monitoring of access made by those users with the System Administrator role profile to confirm that it is appropriate.

We are aware that the ISD team is liaising with NGA to improve reporting capability.

Management Action Plan

The ISD team has secured improved reporting capability and will continue to provide audit logs as and when requested.

Importance:	Low
Responsible Officer:	S Liston, Team Leader ISD
Lead Service:	Corporate and Democratic Services
Date for Completion (Month / Year):	March 2016
Required Evidence of Completion:	A log to be provided

Auditor’s Comments

Satisfactory