

**The Highland Council**  
**Resources Committee – 25 February 2015**

Agenda Item	<b>11(a)</b>
Report No	<b>RES/12/15</b>

**Internal Audit Report – Review of the Oracle Financials System**

**Report by Director of Finance**

**Summary**

This report provides the outcomes of the Internal Audit's work on the Oracle Financial Management Information System

**1. Background**

- 1.1 The Council currently uses Oracle Financials to manage its supplier payments, miscellaneous income and accounting and financial reporting processes.
- 1.2 A contract has been agreed with Capita to supply a new Financial Management Information System called Integra from 1 April 2015.

**2. Report Findings**

- 2.1 The Internal Audit Report can be found at **Appendix 1** and was presented to the Audit and Scrutiny Committee on 20 November 2014.
- 2.2 The Audit opinion concluded for this review was *Substantial Assurance*.

**3. Audit recommendations**

- 3.1 The Action Plan contains 2 recommendations, graded at *Medium Priority*. *Medium Priority* is described as "important issues that managers should address and will benefit the organisation if implemented".
- 3.2 The recommendations are due to be completed in conjunction with the implementation of Integra.

**4. Implications**

- 4.1 There are no Legal, Equalities, Climate Change/Carbon Clever, Risk, Rural or Gaelic implications arising from this report.

**Recommendation:**

Members are asked to note the findings of the Internal Audit Report on Oracle Financials presented to Audit and Scrutiny Committee on 20 November 2014, and the actions being taken to implement its findings.

Designation:	Director of Finance
Author:	David Robertson, Head of Corporate Finance
Date:	2 February 2015
Attachments:	Appendix 1 – Internal Audit Report



**CONFIDENTIAL**

**INTERNAL AUDIT  
FINAL REPORT**

FINANCE

ORACLE FINANCIALS

**AUTHOR**

David Beaton  
Internal Audit  
Finance Service

**REF:** HK07/014.bf

**DISTRIBUTION**

Director of Finance  
Head of Corporate Finance (for info)  
Audit Scotland (for info)

**DRAFT DATE:** 3/11/14

**FINAL DATE:** 5/11/14

**Contents**

<b>1.</b>	<b>MANAGEMENT SUMMARY .....</b>	<b>1</b>
1.1	INTRODUCTION	1
1.2	REVIEW OBJECTIVES	1
1.3	MAIN FINDINGS	1
1.4	CONCLUSION	1
1.5	AUDIT OPINION	2
<b>2.</b>	<b>SCOPE, METHOD AND COVERAGE.....</b>	<b>3</b>
<b>3.</b>	<b>FINDINGS AND RECOMMENDATIONS.....</b>	<b>4</b>
3.1	ACCESS CONTROL POLICY	4
3.2	PASSWORD COMPLEXITY	4
3.3	APPLICATION CONTROLS	4
<b>4.</b>	<b>ACTION PLAN .....</b>	<b>5</b>

## **1. MANAGEMENT SUMMARY**

### **1.1 Introduction**

The Oracle Financial Management Information System is currently used to manage the Council's income, expenditure and accounts. The Council's revenue budget of almost £564 million, and the capital budget was just over £78 million for financial year 2014/15, are controlled using this system. This system is to be replaced on 1 April 2015, by the new Integra Financial Management Information System. Therefore the findings and actions resulting from this audit will be implemented for the new system, not the existing one.

The audit was included as part of the 2013 2014 Audit Plan.

### **1.2 Review Objectives**

Given the system is to be replaced in April 2015, the objectives of the review were restricted to the following areas to ensure that:

- (i) Logical access controls in terms of policy and passwords comply with expected best practice
- (ii) Application controls in terms of the update of standing data such as account codes; processing of interface data to and from the Oracle Financials System; and electronic audit trail recording are satisfactory.

The review checked the procedures for updating standing data and processing interfaces. In addition audit trail reports were run to ensure they contained the expected data.

The scope of this review did not include controls surrounding general transaction data input or the output of transaction reports.

### **1.3 Main Findings**

The main findings of the review, referenced to the above review objectives, are as follows:

- (i) This objective was mainly achieved. A draft Access Control Policy and a formal User Registration System are in place (section 3.1). Password complexity controls are only partially set up and enforced in that the user must enter a password that is a minimum of 6 characters long, but it does not need to contain a mixture of letters and numbers or upper and lower case letters (section 3.2).
- (ii) This objective was fully achieved. The Finance Systems Administration Team have a well documented procedure for setting up standing data such as account codes which ensures they need to be properly authorised. It also has good documented procedures in place for interface processing which include documented reconciliation checks and procedures for handling known errors. The sign-on audit trail of user logins and the manually configured table level audit trail showing all important user transactions are both operating as expected.

### **1.4 Conclusion**

The controls checked were mainly satisfactory and the Finance Systems Administration Team operating procedures that were examined during the review are of a good standard. The two improvements identified, which are to be applied to the new Integra System, should assist with a successful implementation.

There are 2 recommendations in this report. Both are classified as medium priority and are due to implemented by the start of April 2015.

### **1.5 Audit Opinion**

The opinion is based upon, and limited to, the work performed in respect of the subject under review. Internal Audit cannot provide total assurance that control weaknesses or irregularities do not exist. It is the opinion that **Substantial Assurance** can be given in that while there is generally a sound system, there are minor areas of weakness which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk. The levels of assurance and their definitions can be found at Appendix 1.

## **2. SCOPE, METHOD AND COVERAGE**

2.1 The areas to be reviewed within each objective are as follows:

(i) Access Controls

- The access control policy and user registration system used to control logical access to oracle Financials
- How password controls are set up and enforced

(ii) Application Controls

- The procedures used for standing data input, e.g. ledger codes, to ensure it is authorised, complete, accurate and timely
- The procedures used for interface processing to ensure that it is checked to be complete and accurate
- The electronic audit trails which record user logons and important transactions to ensure they are set up and provide sufficient detail for monitoring user activity The review will not include controls surrounding transactional data input or the output of reports.

2.2 The existing Access Control Policy was reviewed as was the procedure for giving a member of staff access to the system. The system settings for password controls were also examined. The documented procedures used to set up account codes and to process three interfaces were also examined. Finally audits reports of user logins and important transactions were run and the output was checked to be as expected.

2.3 Staff involved in the audit were:

- Finance Manager (Corporate Budgeting, Treasury and Taxation)
- Members of the Finance Systems Administration Team.

Thanks are extended to all of these officers for their courtesy, co-operation and assistance in this assignment.

### **3. FINDINGS AND RECOMMENDATIONS**

#### **3.1 Access Control Policy**

A draft Access Control Policy was produced in 2006, but it has not yet been completed and approved.

**Recommendation:**

A new Access Control Policy should be produced when the new Integra System is introduced and it should be formally approved.

#### **3.2 Password Complexity**

The system only forces the user to put in a minimum of 6 characters. It does not force mixed case or a mix of numbers/special characters and letters. It does not prevent re-use of passwords. The facility to make passwords hard to guess has not been switched on.

**Recommendation:**

Password complexity should be enforced when the new Integra System is introduced. It is understood there is functionality within the new system to do this.

#### **3.3 Application Controls**

The documented procedures used to set up standing data - which is mainly fixed throughout the lifetime of the system or is only updated annually - were found to be satisfactory. The procedures used to process three interfaces were also found to be satisfactory. The sample sign-on audit trail report and the sample bank account update audit trail report both produced output in line with expectations.



#### 4. ACTION PLAN

The Action Plan contains 2 recommendations as follows:

Description	Priority	Number
Major issues that managers need to address as a matter of urgency.	High	0
Important issues that managers should address and will benefit the Organisation if implemented.	Medium	2
Minor issues that are not critical but managers should address.	Low	0
<b>Total recommendations</b>		<b>2</b>

REPORT REF.	GRADE	FINDING	RECOMMENDATION	MANAGEMENT AGREED ACTION	IMPLEMENTATION	
					RESPONSIBLE OFFICER	TARGET DATE
3.1	Medium	A draft Access Control Policy was produced in 2006, but it has not yet been completed and approved.	A new Access Control Policy should be produced when the new Integra System is introduced and it should be formally approved.	A new Access Control Policy will be produced as part of the Integra project.	Finance Manager (Corporate Budgeting, Treasury and Taxation)	01/04/15
3.2	Medium	The system only forces the user to put in a minimum of 6 characters. It does not force mixed case or a mix of numbers/special characters and letters. It does not prevent re-use of passwords. The facility to make passwords hard to guess has not been switched on.	Password complexity should be enforced when the new Integra System is introduced. It is understood there is functionality within the new system to do this.	Integra password setting allows the Council to design password complexity at corporate level and user level.	Finance Manager (Corporate Budgeting, Treasury and Taxation)	01/04/15

**Internal Audit Opinion**

<b>Level</b>	<b>Definition</b>
<b>Full Assurance</b>	There is a sound system of control designed to achieve the system objectives and the controls are being consistently applied.
<b>Substantial Assurance</b>	While there is generally a sound system, there are minor areas of weakness which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.
<b>Reasonable Assurance</b>	Whilst the system is broadly reliable, areas of weakness have been identified which put some of the system objectives at risk, and/ or there is evidence that the level of non-compliance with some of the controls may put some of the system objectives at risk.
<b>Limited Assurance</b>	Weaknesses in the system of controls are such as to put the system objectives at risk, and/ or the level of non-compliance puts the system objectives at risk.
<b>No Assurance</b>	Control is generally weak, leaving the system open to significant error or abuse, and/ or significant non-compliance with basic controls leaves the system open to error or abuse.