Committee report

Core financial systems review of creditors standing data

Committee Audit and Standards

Date of meeting 8 June 2018 **Date of report** 23 May 2018

Report by Assistant Chief Executive

1. Object of report

To advise the committee on the findings of a core financial systems review of creditors standing data. This engagement is included in the annual Internal Audit plan for 2017/18.

2. Background

SPT pays creditors for a wide range of goods and services to support the delivery of strategic priorities.

Standing data is master file information held in a database for long term use i.e. registered company names, address details, banking information which in practice, does not change regularly. This data is used to process payments to creditors.

Documented procedural guidance is in place for Finance & HR staff assigned to add new or amend creditor standing data (including) bank account details held in the Technology One Financial Management System (T1).

The objective of this engagement was to undertake an integrity check on payroll and creditors bank details and evaluate the current processes and procedures in place for changing bank account details/standing data.

This engagement tested elements of the internal controls and mitigation against SPT 22: Governance arrangements, as identified in the Corporate Risk register.

3. Outline of findings

Engagement testing (January 2018) found a protocol in place for adding new employees and creditors to the corporate financial management system (T1) and for amending existing information.

New information and amendments to existing creditor standing data can only be made by designated individuals after receipt of supporting documentation and completion of a

validation process. An output report is generated from the T1 system to allow substantive checks to be carried out on new records and changes to standing data.

A key internal control in the current system is that payment to creditor(s) is made by cheque until changes to bank account details have been validated.

Creditors and employee and member standing data (bank account matching) testing indicated payments were being made through the correct system(s) with no matches between the two systems.

The engagement identified a requirement for Finance management to review system roles, responsibilities and privileges.

There are areas for improvement, and these areas have been addressed by two audit recommendations. Finance management have agreed to implement these recommendations, which are currently being actioned.

4. Conclusions

The Audit and Assurance team has undertaken a core financial systems review of creditors standing data. Two recommendations have been agreed from this engagement.

Key controls exist and are applied consistently and effectively in the majority of areas tested in this engagement. Reasonable assurance can be taken from the controls in place for the areas covered in this engagement.

5. Committee action

The committee is asked to note the contents of this report and agree that the Audit and Assurance Manager submits a follow-up report on the implementation of the recommendations to a meeting in approximately six months.

6. Consequences

Policy consequences	*None*
Legal consequences	*None*
Financial consequences	*None*
Personnel consequences	*None*
Social Inclusion consequences	*None*
Risk consequences	*As detailed in the report*

Name	Valerie Davidson	**Name**	Gordon Maclennan
Title	**Assistant Chief Executive**	**Title**	**Chief Executive**

For further information, please contact Iain McNicol, Audit and Assurance Manager on 0141 333 3195.

Agreed action plan: core financial systems review of creditors standing data

No.	Recommendation	Priority	Action Proposed	Lead Officer	Due date
1.	<u>Financial management system access</u> Finance management should: • change the financial management system access password(s) before and after authorised use by consultant(s)/Digital staff; and • on a regular a basis (i.e. every period) check Digital user activity to ensure no unauthorised activity or changes have been made.	High	System access password(s) will be changed before and after each session by consultants/ Digital staff. An exceptions report (Business Intelligence report) will be created and checked each (financial) period.	Chief Accountant	January 2018
2.	<u>Payroll system (Chris[21]) access</u> Finance management should review the following internal controls: • documented procedures/ guidelines for designated staff making changes to payroll standing data including bank account details; • produce a report which allows any changes to payroll and supplier standing data including bank account details to be obtained directly from the system(s). The notification/exceptions report should be reviewed and checked as required to ensure no unauthorised bank account changes are being made; • roles and responsibilities together with system privileges should be reviewed to ensure adequate separation of duties.	Medium	Current procedural guidance will be reviewed/updated, where appropriate. An exceptions report will be created and reviewed each (financial) period. Roles and responsibilities and system privileges will be reviewed.	Chief Accountant	February 2018

High – A fundamental control that should be addressed as soon as possible;
Medium – An important control that should be addressed as a priority;
Low – An issue which is not fundamental but would improve overall control.