

Internal Audit and Counter Fraud Quarter 3 Progress Report 2018/19

CONTENTS

1. Summary of Completed Audits
2. Counter Fraud and Investigation Activities
3. Action Tracking
4. Amendments to the Audit Plan
5. Internal Audit Performance

1. Summary of Completed Audits

Accounts Payable

- 1.1 This is the first occasion that the Technology One system has been in operation for a full year and officers now have a clearer understanding of how the system operates.
- 1.2 The purpose of the audit was to provide assurance that:
- Orders are raised for goods, works and services for bona fide services in accordance with standard financial procedures.
 - All payments (including non-order invoices, cheque requisitions and urgent payments where appropriate) are subject to review and approval to ensure payments are valid and goods, works or services have been received and are correctly processed.
 - Payment runs are subject to appropriate review and authorisation.
 - Only creditors that meet the needs of the Council and that do not already exist in the Financial Information System (FIS) are set up. All creditors' details are maintained accurately within the FIS.
 - Transactions in the Accounts Payable system are completely and accurately transferred to (or reflected in) the General Ledger
- 1.3 As a result of this work, we were able to provide **substantial assurance** over the controls operating within the area under review. The Technology One system has effective processes in place for logging any changes that are made to requisitions, orders, and invoices. The workflow system allowed the auditor to obtain evidence from the system as required. There is a clear "audit trail" of who has entered, amended or authorised orders and invoices within the system.
- 1.4 Only one minor area for improvement was identified and agreed, which was for the purpose of improving efficiency.

Performance Management

- 1.5 At the time of the audit, a new basket of indicators was being developed to measure strategic performance in key areas. The audit reviewed the performance management framework and a sample of key performance indicators was tested for accuracy.
- 1.6 The purpose of the review was to provide assurance that:
- There is an effective framework for performance management, including the development of a set of SMART key performance measures based on strategic and departmental objectives.
 - Key performance indicators (KPIs) are calculated consistently and correctly on the basis of clear definitions and that the information is recorded on the corporate 'Pentana' system in a timely manner.
 - Effective systems are in place for monitoring and reporting on performance management and that actions are taken as necessary to deal with any deteriorating performance.
 - Managers are fully engaged and accountable in the monitoring and use of KPIs.

- 1.7 Overall, we were able to provide **reasonable assurance** over the controls operating within the area under review. The Council has a well-established performance management framework that covers the annual agreement of a 'basket' of KPIs that are linked to the Council's strategic objectives. A quarterly report is submitted to the Overview and Scrutiny Committee for consideration by Members.
- 1.8 Area for improvement:
- A few areas for improvement were identified in relation to key performance indicators and how they are used to support service improvement.

Cyber Security

- 1.9 This audit was carried out to review the effectiveness of the Council's control processes that have been designed to mitigate cyber security attacks. It is widely recognised that even with the most effective control processes in place an organisation cannot prevent cyber-attacks. It is important, therefore, that robust control processes are introduced to minimise the impact and damage caused by such an attack on the operations of the Council.
- 1.10 The purpose of the review was to ensure:
- The Council has a communicated "Information Risk Management Regime" that is central to its overall cyber security strategy.
 - The Council applies secure configuration of all IT systems.
 - The Council employs appropriate protection to the perimeter to reduce the threat of unauthorised remote access to the Council's network.
 - The Council has effective management processes in place to limit the number of privileged accounts, control user privileges and monitor user activity.
 - User security policies are in place and all officers and councillors have received cyber-security training and are aware of their role in supporting the authority in managing cyber security threats.
 - Anti-malware defences have been introduced, including filtering web access and scanning for malware across Council systems, designed to discover remove and reduce the possibility of damage to Council systems.
 - A secure baseline build has been introduced for all devices to protect data both in transit and at rest.
 - Arrangements are in place to identify developing trends and emerging threats, ensuring that the information is obtained from respected national sources.
- 1.11 Overall, we were able to provide **reasonable assurance** over the controls operating within the area under review. Reliance was placed upon the testing carried out by third party specialists, SureCloud, which demonstrated that the Council met the specific security requirements for the Code of Connection for PSN¹. The IT Health Check (ITHC) report produced by SureCloud provides assurance, upon which we could rely, for key areas within the scope of this audit, including firewall security; patch management; network controls; and the secure configuration of Council Desktop PCs & Laptop computers.

¹ PSN = Public Services Network, the government's high performance network which helps public sector organisations work together and share resources. In order to connect to this network, organisations must provide evidence that they have effective security controls in place to meet the "Code of Connection" (CoCo).

- 1.12 Internal Audit focused its work on the areas that are outside of the remit of the PSN Code of Connection and the ITHC report. The auditor identified that whilst the IT Technical Services team has carried out significant work in securing the IT infrastructure, the Council has placed less emphasis on identifying and mitigating risks posed by the actions of users. Action is now being taken to address these particular weaknesses. The Head of Technology Services has updated and revised the Council's Information Security Policies and work is also being carried out to promote awareness of cyber security threats and to introduce mandatory training for staff.

Health and Safety

- 1.13 The Council has a statutory duty under the Health and Safety at Work Act 1974 (the Act) to secure, as far as is reasonably practicable, the health and safety of employees and others who may be affected by the Council's activities. Serious harm to an employee or a service user can result in significant costs to the Council as well as the possibility of reputational damage. There are also individual responsibilities under the Act. Failure of individuals and organisations to comply can lead to unlimited fines and possible imprisonment. The importance of effective health and safety management has become even more crucial with the introduction of the offence of corporate manslaughter.
- 1.14 The Health and Safety Executive (HSE) has developed a framework (Health and Safety Guidance 65: Successful Health and Safety Management) to help organisations understand the actions that they need to take to comply with health and safety legislation. The requirements set out in the HSE framework are expected to be tailored to individual organisation's circumstances, and the HSE advocates a practical approach that seeks a balance between the unachievable aim of absolute safety, and poor management of safety that puts people at risk
- 1.15 The objectives of the review were as follows:
- To ensure there is effective management to help protect the health and safety of employees, service users, suppliers and members of the public who interact with the Council, so far as is reasonably practicable.
 - To ensure that there are effective arrangements in place that makes the Council a safe and healthy place for employees, service users, suppliers and members of the public who interact with the Council.
 - To ensure that there is sufficient evidence in place to demonstrate that the Council is doing what it needs to do to manage health and safety in accordance with legislation.
- 1.16 Overall, we were able to provide **reasonable assurance** over the controls operating within the area under review. A corporate health and safety policy is in place; roles and responsibilities for relevant aspects of health and safety have been defined and allocated appropriately; the Council has adopted a risk based approach to managing health and safety; there are arrangements in place (i.e. routine safety audits and inspections) to actively check to ensure that safety control measures are working properly; a wide range of health and safety training courses have been made available to staff; and SLT receives an update on health and safety matters on a regular basis.
- 1.17 The following areas for improvement have also been identified and agreed with management as part of the audit:
- Plans to continuously improve health and safety will be developed.

- Senior Management and staff will be encouraged to improve their uptake of mandatory health and safety training.
- The policy for the management of health and safety when selecting and managing contractors will be reviewed.
- The Corporate Health and Safety Management Forum will monitor and review risk assessments relating to activities that it considers to be of priority and/or exposes the Council to the greatest health and safety risks/issues.
- IT solutions for recording risk assessments will be explored.
- Performance indicators will be developed to improve health and safety performance monitoring.

Treasury Management

- 1.18 This routine review has been undertaken to ensure that the Treasury function is operating within the confines of the Treasury Management Strategy and Prudential Code.
- 1.19 Horsham DC had a balance of £44 million in investments at the time of the audit. No short term borrowing has been entered into during the financial year to date.
- 1.20 The purpose of the audit was to provide assurance that controls are in place to meet the following objectives:
- The Council has established an appropriate Treasury Management Policy & Investment Strategy;
 - All lending and borrowing decisions are based on robust cash flow forecasting over the short, medium and long term;
 - Investments are made with approved counterparties within approved limits, are correctly paid, authorised, and are repaid by counterparties with the correct amount of interest;
 - Borrowings are made only from approved organisations, are correctly authorised and repaid to counterparties with the correct amount of interest;
 - There is regular and independent reconciliation between the Treasury Management record, the Bank Account and the General Ledger;
 - Officers and elected Members receive regular and informative training and performance monitoring information.
- 1.21 Overall, we were able to provide **reasonable assurance** over the controls operating within the area under review. This is demonstrated by the following points:
- The Council's Cash Flow is reviewed and updated daily. The forecast is used to enable sensible investment decisions to be made so that funds are available when needed and investments are placed appropriately.
 - Monthly meetings are held between the Director of Corporate Resources, the Head of Finance and the Group Accountant (Technical) to review Treasury Management performance for the period, consider risk areas and discuss any major proposed transactions. These meetings provide strategic management and are routinely minuted. Plans are being made to produce a Capital Strategy document for consideration by Members in accordance with the new CIPFA Treasury Management Code 2017.

- Day to day transactions are mainly undertaken by a single experienced officer, supported by senior officer oversight at an appropriate level. Monthly reconciliations are carried out, and these are reviewed and verified by the Group Accountant (Technical).
- The Group Accountant (Technical) regularly attends briefings provided by CIPFA and by the Council's Treasury Management Advisors (Arlingclose) in order to keep up to date on emerging issues.

1.22 There was only one area for improvement identified. Audit testing of a sample of ten investment decisions showed that in one instance the audit trail for the CHAPS payment was not complete. Because the current system requires that the audit trail is recorded on paper documents that are then copied and filed electronically, care is needed to ensure that the record is complete. The monthly reconciliations are also complex and it would not be easy for another member of staff to undertake these duties if the regular post holder were absent. Senior Management has agreed to make plans to provide cover arrangements for this area.

IR35 (Off-Payroll Engagement)

1.23 The tax year that began on 6th April 2017 saw changes to intermediaries' legislation, known as IR35, for off-payroll working in the public sector. Where IR35 rules apply, people who work through an intermediary (such as a personal service company) will pay employment taxes in a similar way to employees. One notable change is that responsibility for deciding whether or not IR35 rules apply to off-payroll engagements has shifted on to the public authority itself. Consequently, the Council has decided that all engagements should be paid for through payroll unless it can be justified or evidenced otherwise. This message has been communicated to service managers and processes have been put in place to identify the correct IR35 status for off-payroll workers.

1.24 The purpose of the audit was to provide assurance that controls are in place to meet the following objectives:

- The correct IR35 tax status is determined for all off-payroll engagements, either engaged directly by the council or through an agency;
- Off payroll engagements made by the council are readily identifiable and paid in compliance with IR35 legislation and council policy;
- Off payroll engagements are made in line with procurement processes to ensure value for money is achieved.

1.25 Overall, we were able to provide **substantial assurance** over the controls operating within the area under review because:

- The Council has responded pro-actively to the changes made to IR35 legislation, engaging extensively with service managers and introducing a number of controls to manage the risks associated with IR35 and off-payroll engagements.
- Effective leadership has been demonstrated through the adoption of a clear position, which has been well communicated to all key stakeholders.
- Processes are in place and operating effectively to ensure the correct IR35 tax arrangements are in place for off-payroll engagements before any payment is released.

- 1.26 A few areas for improvement were identified, including that IR35 requirements should be made available on the Council's Intranet site to help to further raise awareness of IR35 rules for off-payroll engagements.

2. Counter Fraud and Investigation Activities

Proactive Counter Fraud Work

- 2.1 The Orbis Internal Audit structure came into effect from 1st April 2018. The integrated structure was designed to deliver resilience, flexibility and quality, along with specific specialisms. A key strand of the structure was the formation of a counter fraud team that would deliver both reactive and proactive fraud services across the partnership. Work to date has focussed on the following areas:

National Fraud Initiative Exercise

- 2.2 The results from this exercise were received on 31 January 2018 and will be prioritised for review over the coming months.

Fraud Risk Assessments

- 2.3 A Fraud risk assessment has been undertaken to ensure that the current fraud threat for the Council has been considered and appropriate mitigating actions identified.

Fraud Response Plans

- 2.4 Fraud Response Plans take into consideration the fraud risk assessments and emerging trends across the public sector in order to provide a proactive counter fraud programme. These are being reviewed and aligned to deliver an efficient and effective programme of work across the Orbis partners. This will include an increased emphasis on data analytics. The Fraud Response Plans will set out the proactive work plan for the team in 2019/20.

3. Action Tracking

- 3.1 All high and medium priority actions agreed with management as part of individual audit reviews are subject to action tracking. As at the end of quarter 3, 97% of high priority actions due had been implemented within agreed timescales.

- 3.2 Implementation of high and medium priority agreed audit actions (based on a 12 month rolling period):

Period to:	High & Medium Priority Agreed Actions Due	Not implemented	Implemented	% Implemented
31/12/18	35	1	34	97%

- 3.3 Internal Audit will continue to work with senior management to ensure that sufficient attention is given to actions that remain overdue and an update on progress will continue to be reported to this committee.

3.4 Details of outstanding priority agreed action:

Audit / Agreed Action	Directorate	Due Date	Revised Date	Progress to date
<p>Medium Priority <i>Creditors:</i></p> <p>Purchase Orders raised as a percentage of invoices received:</p> <p>A target of 60% has been re-introduced for 2017/18 and will be reported within the performance indicators to the Finance and Performance Committee on a quarterly basis.</p>	<p>Corporate Resources</p>	<p>31/12/17</p>	<p>31/03/19</p>	<p><u>March 2019 Management Update:</u></p> <p>This has not been addressed as other areas of work within Finance have taken a higher priority (for example, Green Waste income collection, the automation of revenue and capital accounting, and accounts receivable).</p> <p>The current process of using Purchase Orders is cumbersome and inefficient. It does not encourage users to do this, especially for 'multiple' deliveries. This needs a lot of time spending to redesign.</p> <p>The Finance team is also planning to review the functionality within AP for intelligent processing software once other priority closedown and accounts work has completed.</p>

4. Amendments to the Audit Plan

4.1 In accordance with proper professional practice, the internal audit plan for the year remains under regular review to ensure that the service continues to focus its resources in the highest priority areas based on an assessment of risk. Through discussions with management, the following reviews have been added to the audit plan during the year:

- Housing Benefits Subsidy – Lessons Learnt
- Review of bomb / lockdown procedures for Parkside and buildings owned by Horsham D.C.
- Input to the review of the Council’s Constitution
- Review of Housing Company Business Case
- Review of Information Security Policy Suite
- Advice and data analytics work to support the implementation of the new Technology One HR system

4.2 Through the same process, the following audits have been removed or deferred from the audit plan and, where appropriate, will be considered for inclusion in the 2019/20 plan as part of the overall risk assessment completed during the annual audit planning process:

- Contracts - Procurement (as reported in October).
- ICT Service Desk (as reported in December)
- General Data Protection Regulations (GDPR) – postponed until May 2019 following the resignation of the Information Governance Officer.

5. Internal Audit Performance

5.1 In addition to the annual assessment of internal audit effectiveness against Public Sector Internal Audit Standards (PSIAS), the performance of the service is monitored on an ongoing basis against a set up agreed key performance indicators as set out in the following table:

Aspect of Service	Orbis IA KPI	Target	RAG score	Actual Performance
Quality	Annual Audit Plan agreed by Audit Committee	By end April	G	Approved by Audit Committee on 11 April 2018
	Annual Audit Report and Opinion	By end July	G	2017/18 report approved by Committee on 12/07/18
	Customer Satisfaction levels	90% satisfied	G	100%
Productivity and process efficiency	Audit Plan – completion to draft report stage	90%	G	78% completed to draft report stage by end of Q3 (against a Q3 target of 67.5%)
Compliance with professional standards	Public Sector Internal Audit Standards complied with	Conforms	G	January 2018 - External assessment by the South West Audit Partnership gave an opinion of 'Generally Conforms' – the highest of three possible rankings
	Relevant legislation such as the Police And Criminal Evidence Act, Criminal Procedures and Investigations Act	Conforms	G	No evidence of non-compliance identified
Outcome and degree of influence	Implementation of management actions agreed in response to audit findings	95% for high & Medium priority agreed actions	G	97%
Our staff	Professionally qualified / accredited	80%	G	85% ²

² Includes part-qualified staff

Audit Opinions and Definitions

Opinion	Definition
Substantial Assurance	Controls are in place and are operating as expected to manage key risks to the achievement of system or service objectives.
Reasonable Assurance	Most controls are in place and are operating as expected to manage key risks to the achievement of system or service objectives.
Partial Assurance	There are weaknesses in the system of control and/or the level of non-compliance is such as to put the achievement of the system or service objectives at risk.
Minimal Assurance	Controls are generally weak or non-existent, leaving the system open to the risk of significant error or fraud. There is a high risk to the ability of the system/service to meet its objectives.