SWAP
SOUTH WEST AUDIT PARTNERSHIP
Delivering Audit Excellence

South Somerset District Council

Report of Internal Audit Activity

Plan Progress 2017/18 up to 31 January 2018

Internal Audit ▪ Risk ▪ Special Investigations ▪ Consultancy

Contents

The contacts at SWAP in connection with this report are:

Gerry Cox
Chief Executive
Tel: 01935 385906
gerry.cox@southwestaudit.co.uk

Ian Baker
Director of Quality
Tel: 01935 385906
ian.baker@southwestaudit.co.uk

Laura Wicks
Senior Auditor
Tel: 01935 385906
laura.wicks@southwestaudit.co.uk

Internal Audit Plan Progress 2017/18

Our audit activity is split between:

- **Operational Audit**
- **School Themes**
- **Governance Audit**
- **Key Control Audit**
- **IT Audit**
- **Grants**
- **Other Reviews**

Role of Internal Audit

The Internal Audit service for the South Somerset District Council is provided by South West Audit Partnership Limited (SWAP). SWAP is a Local Authority controlled Company. SWAP has adopted and works to the Standards of the Institute of Internal Auditors, further guided by interpretation provided by the Public Sector Internal Audit Standards (PSIAS), and also follows the CIPFA Code of Practice for Internal Audit. The Partnership is also guided by the Internal Audit Charter which was approved by the Audit Committee at its meeting on 22 June 2017.

Internal Audit provides an independent and objective opinion on the Authority's control environment by evaluating its effectiveness. Primarily the work includes:

- Operational Audit Reviews
- Cross Cutting Governance Audits
- IT Audits
- Grants
- Other Special or Unplanned Reviews

Internal Audit work is largely driven by an Annual Audit Plan. This is approved by the Section 151 Officer, following consultation with the Senior Leadership Team and External Auditors. This year's Audit Plan was reported to this Committee and approved at its meeting in March 2017.

Audit assignments are undertaken in accordance with this Plan to assess current levels of governance, control and risk.

Outturn to Date:

We rank our recommendations on a scale of 1 to 5, with 1 being minor or administrative concerns to 5 being areas of major concern requiring immediate corrective action

Internal Audit Work Programme

The schedule provided at Appendix B contains a list of all audits as agreed in the Annual Audit Plan 2017/18. I am pleased to report with the finalising of the Healthy Organisation report that the 2016/17 plan is completed.

It is important that Members are aware of the status of all audits and that this information helps them place reliance on the work of Internal Audit and its ability to complete the plan as agreed.

Each completed assignment includes its respective "assurance opinion" rating together with the number and relative ranking of recommendations that have been raised with management. In such cases, the Committee can take assurance that improvement actions have been agreed with management to address these. The assurance opinion ratings have been determined in accordance with the Internal Audit "Audit Framework Definitions" as detailed in Appendix A.

In the period Quarter 3 to 31 January 2018 the following audits have been completed from the 2017/18 Audit Plan:

- Cyber Security
- Grant Funding Fraud Audit
- Creditors
- Payroll
- Cash Receipting

The following Audits are in progress at the time of writing this report and a verbal update will be provided to the Committee on these:

2017/18 Audit Plan

- Organised Crime checklist – In progress
- Housing Benefit Claim/Subsidy – In Progress
- Elections – In Progress
- Transformation Support Q3 & Q4 – In Progress – to focus on: Governance of Service Redesign, Financial Services Processes Redesign, General Data Protection Regulations (GDPR) and Business as Usual.

Outturn to Date: continued……

To assist the Committee in its important monitoring and scrutiny role, in those cases where weaknesses have been identified in service/function reviews that are considered to represent significant service risks, a summary of the key audit findings that have resulted in them receiving a 'Partial Assurance Opinion' are reported; there are no Partial Opinion reports this time. However, whilst a Reasonable assurance opinion was offered on the Cyber Security report, a significant risk was highlighted therein: Lack of strategy and engagement with stakeholders to outline the security of the organisation's digital infrastructure, cyber attacks occur, data is lost, impacting on the stability of the organisation and its reputation. The weaknesses found in this report are outlined with Appendix C.

Added Value

Extra feature(s) of an item of interest (product, service, person etc.) that go beyond the standard expectations and provide something more while adding little or nothing to its cost.

Added Value

Primarily Internal Audit is an assurance function and will remain as such. However, Members requested that we provide them with examples of where we have "added value" to a particular service or function under review. In response to this we have changed our approach and internal processes and will now formally capture at the end of each audit where we have "added value".

The SWAP definition of "added value" is "it refers to extra feature(s) of an item of interest (product, service, person etc.) that go beyond the standard expectations and provide something "more" while adding little or nothing to its cost".

During Quarter 3 to 31 January 2018, we have sought to add value as follows to the 2017/18 audit plan:

- In revisiting the 2017/18 audit plan and through the provision of support during the Transformation Project, it was agreed in a meeting with the Section 151 Officer and Strategic Transformation Lead to focus on the areas deemed of highest risk: Governance of Service Redesign, Financial Services Processes Redesign, General Data Protection Regulations (GDPR) and Business as Usual (concentrating on the management of impacts to services through Transformation.
- We have developed a GDPR 'Self-Assessment' template for the Authority to utilise in determining its readiness to comply with the new legislation, which is based on a work programme used at other SWAP Partners. The programme takes a 'gap analysis' approach and should serve to highlight the areas where the Authority needs to focus its efforts in order to achieve compliance. This 'Self-Assessment' was also supported by benchmarking data obtained from our Partners to provide a frame of reference of progress towards compliance.
- We have completed a number of reviews to provide assurance on potential risk areas for fraud.
- The Elections audit will be undertaken on a joint basis with East Devon District Council in order to share best practice.

We keep our audit plans under regular review so as to ensure that we auditing the right things at the right time.

Approved Changes to the Audit Plan

The following changes have been made to the audit plan in Quarter 3 to 31 January 2018 to ensure internal audit resources are focused on the key risks faced by the Council. All changes are made in agreement with or at the request of the Section 151 Officer:

As stated above, it has been agreed to utilise the remaining annual plan days to provide support to the Transformation project. In order to facilitate this, we have kept some core audits in the plan for quarters 3 and 4 but removed others (See Appendix B). This will ensure that assurance is focused on the areas of greater risk to the organisation. The areas of focus, which are aligned to the areas of greater risk during the Transformation Programme, are outlined above. As this work is ongoing, a verbal update will be provided at the meeting of the Audit Committee on 22 February 2018.

In addition, following the findings from Grant Thornton's report on the Authority's Housing Benefit Subsidy, in agreement with the Section 151 Officer, we will still undertake a review albeit on a reduced scope as no significant issues were identified.

Due to the ongoing Transformation Programme and the recent finalisation of the Healthy Organisation 2016/17 programme of work, it has been proposed that the Risk Management Follow Up 2017/18 work is deferred for inclusion in the 2018/19 audit plan.

At the conclusion of audit assignment work each review is awarded a "Control Assurance Definition";

- **Substantial**
- **Reasonable**
- **Partial**
- **None**

Audit Framework Definitions

Control Assurance Definitions

Substantial	▲★★★	I am able to offer substantial assurance as the areas reviewed were found to be adequately controlled. Internal controls are in place and operating effectively and risks against the achievement of objectives are well managed.
Reasonable	▲★★☆	I am able to offer reasonable assurance as most of the areas reviewed were found to be adequately controlled. Generally risks are well managed but some systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
Partial	▲★☆☆	I am able to offer Partial assurance in relation to the areas reviewed and the controls found to be in place. Some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
None	▲☆☆☆	I am not able to offer any assurance. The areas reviewed were found to be inadequately controlled. Risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.

Categorisation of Recommendations

When making recommendations to Management it is important that they know how important the recommendation is to their service. There should be a clear distinction between how we evaluate the risks identified for the service but scored at a corporate level and the priority assigned to the recommendation. No timeframes have been applied to each Priority as implementation will depend on several factors; however, the definitions imply the importance.

We keep our audit plans under regular review, so as to ensure we are auditing the right things at the right time.

Audit Framework Definitions

- Priority 5: Findings that are fundamental to the integrity of the unit’s business processes and require the immediate attention of management.
- Priority 4: Important findings that need to be resolved by management.
- Priority 3: The accuracy of records is at risk and requires attention.
- Priority 2: Minor control issues have been identified which nevertheless need to be addressed.
- Priority 1: Administrative errors identified that should be corrected. Simple, no-cost measures would serve to enhance an existing control.

Definitions of Risk

Risk	Reporting Implications
Low	Issues of a minor nature or best practice where some improvement can be made.
Medium	Issues which should be addressed by management in their areas of responsibility.
High	Issues that we consider need to be brought to the attention of senior management.
Very High	Issues that we consider need to be brought to the attention of both senior management and the Audit Committee.

Audit Type	Audit Area	Quarter	Status	Opinion	No of Rec	5 = Major		↔		1 = Minor
						Recommendation				
						5	4	3	2	1
2017/18										
Grant Certification	Boden Mill & Chard Regeneration Scheme Statement of Accounts	1	Final	Non Opinion	0	0	0	0	0	0
Operational	Yeovil Cemetery & Crematorium Annual Accounts	1	Final	Non Opinion	1	0	0	1	0	0
Operational	Licensing	1	Final	Reasonable	3	0	0	3	0	0
Key Control	Treasury Management	3	Final	Substantial	0	0	0	0	0	0
Governance, Fraud & Corruption	Business Rates Fraud Audit	3	Final	Reasonable	2	0	0	2	0	0
ICT	Cyber security	1	Final	Reasonable	3	0	1	2	0	0
Follow Up	Risk Management Follow Up	2	Not Started		0	0	0	0	0	0
Governance, Fraud & Corruption	Grant Funding Fraud Audit	2	Final	Substantial	2	0	0	2	0	0
Governance, Fraud & Corruption	Organised Crime checklist	2	In Progress		0	0	0	0	0	0
Key Control	Creditors	3	Final	Reasonable	1	0	0	1	0	0
Key Control	Cash Receipting	3	Final	Reasonable	4	0	0	4	0	0
Key Control	Payroll	3	Final	Substantial	0	0	0	0	0	0
Operational	Transformational Support Q3 & Q4	3	In Progress		0	0	0	0	0	0
Operational	Housing Benefit Claims/Subsidy	4	In Progress		0	0	0	0	0	0

Audit Type	Audit Area	Quarter	Status	Opinion	No of Rec	5 = Major	⟷	1 = Minor		
						Recommendation				
						5	4	3	2	1
Operational	Elections	4	In Progress		0	0	0	0	0	0
Operational	Records Management 1718 - SSDC	1	Removed	-	0	0	0	0	0	0
Operational	Risk Management Support 1718 - SSDC	1	Removed	-	0	0	0	0	0	0
Operational	LED contract compliance 1718 - SSDC	3	Removed	-	0	0	0	0	0	0
Operational	Programme and Project Management 1718 - SSDC	3	Removed	-	0	0	0	0	0	0
Operational	Procurement Review 1718 - SSDC	3	Removed	-	0	0	0	0	0	0
Operational	Key Income Streams 1718 - SSDC	4	Removed	-	0	0	0	0	0	0
Operational	S106/ CIL 1718 - SSDC	4	Removed	-	0	0	0	0	0	0
Operational	Accountability 1718 - SSDC	4	Removed	-	0	0	0	0	0	0
Operational	Business Continuity Key Service Test 1718 - SSDC	4	Removed	-	0	0	0	0	0	0

Schedule of potential significant findings identified from Internal Audit work in the period Quarter 3 to 31 January 2018

No	Name of Audit	Weaknesses Found	Risk Identified	Recommendation Action	Managers Agreed Action	Agreed Date of Action
36495	Cyber Security	The ICT Disaster Recovery Plan (DRP) currently does not differentiate between a cyber attack and any other form of ICT outage. The current ICT DR documentation is unsurprisingly focussed on getting the services up and running ASAP. There is not the required level root cause analysis in place prior to the reinstatement of ICT infrastructure and services.	Reinstating the infrastructure and services before performing appropriate Root Cause Analysis may give the malware associated with an initial failure more time to proliferate further throughout the infrastructure, and inappropriately process more data which in turn may lead to increased compromised customer personal information and subsequent financial and reputational damage for the Council.	It has been agreed that the Head of ICT will engage with the relevant parties and ensure that the Disaster Recovery Plan is rewritten to include route cause analysis to identify and quarantine the agents of Cyber Attacks at the earliest opportunity and prior to the reinstatement of infrastructure and services. Roles, responsibilities and contact references for this should be identified and included in this rewording.	The Disaster Recovery Plan will be updated to include how we will respond to a cyber attack to ensure infrastructure and data can be reinstated securely.	31 May 2018
36501	Cyber Security	The logs of network elements, such as: data circuits; routers; firewalls; SolarWinds; etc; are not being used to their fullest extent.	There is a risk that log information that may show early warning of an incident or cyber attack is not being identified and acted upon in a timely manner. This means that a successful cyber attack will be able to compromise more data and there may be greater financial and reputational losses for the Council.	I recommend that the Head of ICT ensures an appropriately skilled resource is allocated to perform tuning on all network metrics/output logs to identify and give increased visibility of cyber security triggers. Using these events and aggregation of these events where applicable, real time, automated controls and person targeted alerts should ensure that timely action is taken in response to the alerts.	Key infrastructure elements are already being monitored and alerts are generated, so we will look at extending this. We will consider each element on a case by case basis and tune the logs and alerts accordingly.	31 July 2018