SWAP
INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

West Oxfordshire District Council

Report of Internal Audit Activity

Summary of Work Completed since March 2021

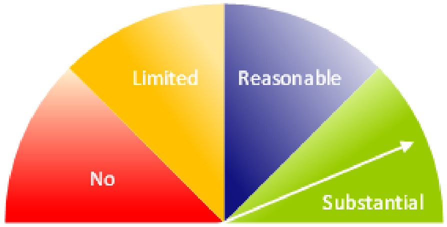
Internal Audit ▪ Risk ▪ Special Investigations ▪ Consultancy

The following information provides a brief summary of each audit review finalised since the last Committee update

Accounts Receivable – Final Audit Report – May 2021

Audit Objective To provide assurance that there is an effective control framework in place within the Accounts Receivable function.

Assurance Opinion



A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

Number of Agreed Actions	
Priority	Number
Priority 1	0
Priority 2	0
Priority 3	0
Total	**0**

Risks Reviewed	Assessment
1. If controls in place in relation to manual allocations of income are not robust, this could result in miss-stating of income, undetected fraud and reputational damage.	Low

Key Findings

The process carried out by the Accounts Receivable (AR) team to identify and allocate income to the correct customer account/invoice from the BAL100 suspense account is robust. As with any manual process there is the possibility of error or mistake, therefore the AR Team Leader has agreed to make quality spot-checks of these manual allocations to ensure the process is followed and payments are allocated correctly.

Continuous Assurance reports were produced on a quarterly basis by the SWAP Data Analytics Team during 2020/21 for Senior Management. In relation to Accounts Receivable, these reports included data relating to the number and value of invoices raised, subscriptions and invoices raised, and value and number of debt write-offs (both in total and by service area) with the aim of identifying any trends or anomalies.

Four recommendations were made in the 2019/20 Accounts Receivable audit. Two of these recommendations are now complete and two are still in progress – due to be complete by October 2021.

Audit Scope

The scope of this audit included a high-level review of the process used by the Accounts Receivable team for the manual allocation of payments from the BAL100 suspense account to customer accounts/invoice and the corresponding investigation process carried out to identify correct customer details.

Recommendations made during the 2019/20 audit were also followed up as part of this work.

In addition to the audit work carried out, the SWAP Data Analytics Team have also provided Continuous Assurance reports (including AR data) quarterly which were provided to Senior Management.

Background

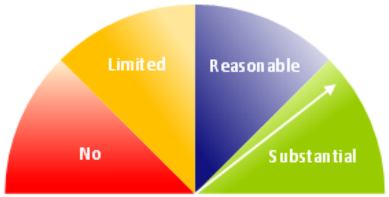
The 2019/20 Accounts Receivable report finalised in August 2020 offered a 'Reasonable' assurance opinion. The current Accounts Receivable Team Leader was appointed in September 2020 and took responsibility for the implementation of the recommendations made during the audit. Added to the impact on staff of the pandemic, it was agreed that the scope of this audit would be focussed on one process.

Main Accounting – Final Audit Report – May 2021

Audit Objective

The objective of the audit is to assess the effectiveness of accounting and budgetary controls and contract management controls operated by service managers, ensuring compliance with financial rules and regulations.

Assurance Opinion



A sound system of governance, risk management and control exists with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

Number of Actions

Priority	Number
Priority 1	0
Priority 2	0
Priority 3	1
Total	**1**

Risks Reviewed	Assessment
1. Ineffective contract management leaves the Council unable to deliver key services putting service users at risk.	Medium
2. Budgetary controls are not robust, so deviations are not identified and corrected.	Low
3. There is greater risk as recommendations have not been implemented.	Low

Key Findings

A survey was issued to a selection of service managers with contract management responsibilities to assess budget monitoring activity undertaken. We did not receive any responses and so we are unable to offer an assurance opinion. The above assurance opinion relates solely to budgetary control activity undertaken by the Finance team.

To ensure a thorough assessment, an audit focussing on Procurement and Contract Performance Management has been included within the 2021/22 audit plan.

There was a delay in uploading opening balances into Business World mainly attributed this year to the delay with External Audit signing off the accounts. However, we identified this same issue in our previous audit. An action has been agreed for balances to be uploaded within one calendar month of the accounts being signed off by the External Auditors.

Budget testing confirmed that the original budget approved by Council balanced with values in Business World. Budget variance testing confirmed variances had been appropriately investigated, reported, and approved. Controls for budget monitoring, virements and reporting were compliant with Financial Rules.

Audit Scope

A review of main accounting controls for the 2020/21 financial year was carried out to assess compliance with Councils' Financial Rules and agreed actions.

The audit covered controls in the following areas:

- Contract management – Service area budget monitoring activity
- Budgetary control, monitoring and reporting
- Balances carried forward
- Previous year's recommendation

Additional Information

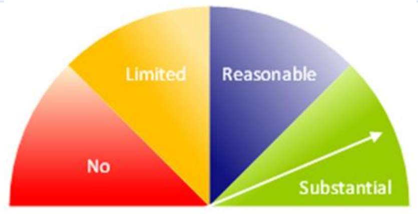
We have identified an unused facility on the In-Tend contract management system that partner councils may wish to consider using to support KPI monitoring responsibilities.

One action has been agreed with management.

Anti-Malware – Final Audit Report – May 2021

Audit Objective To ensure that technical solutions are managed and deployed to protect data and systems from electronic malicious attack.

Assurance Opinion



A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

Number of Agreed Actions

Priority	Number
Priority 1	0
Priority 2	0
Priority 3	1
Total	**1**

Risks Reviewed	Assessment
Operation of the network and connected information systems is disrupted leading to the unauthorised access and disclosure, corruption and loss of information and data.	Medium

Key Findings

We completed an Incident Management audit during 2020/21 which included a review of the response to cyber related threats and incidents. Malware is one such ongoing threat to organisations and as such anti-malware software implementations should be robust, centrally managed and provide maximum coverage of an estate of networked devices. Publica provide ICT support and security defence for the Partner Councils and utilise a 'Next-gen' Anti-Malware solution as part of the strategy to help prevent, detect, contain, and enable the initial response to attacks and infections. 'Next-gen' products are modern solutions for organisations and incorporate enhanced features such as system behavioural monitoring, machine learning and threat intelligence. Device coverage is important, and our review of endpoint installations did identify a small number of discrepancies between the anti-malware solution, Active Directory, and the software management system and whilst these are being remediated, we suggest a periodic compliance check is added to a Security Compliance control diary to ensure these issues are detected, reviewed, and remediated regularly.

Whilst our audit opinion following the assessment of the controls in place has been assessed as 'Substantial' and we take assurance that technical controls are in place and managed appropriately, it is still possible for a malware attack to be successful despite these controls. This can take the form of a '0-day' or 3rd-Party breach such as the 'Solarwinds' attack. It is therefore important the Publica ICT team continue to monitor and manage this risk to continually adapt to the persistent threats facing them and their clients.

Audit Scope

The audit scope reviewed the Anti-Malware solution and considered the following expected key controls:

- Periodic threat assessment to identify current threats and identify remediation required.
- Scanning of in and out-bound communication channels to block viruses, spam, and malware threats.
- Client endpoints are appropriately configured to block viruses, spam, and malware threats.
- Client endpoints are centrally managed and updated, and issues pertaining to connectivity and update failure are identified, reported, and remediated quickly.
- Staff awareness and prevention training.

The review was undertaken by interviewing key personnel including the Cyber Security Engineer and the ICT Audit and Compliance Manager, together with the review of documentation and evidence provided.

Additional Information

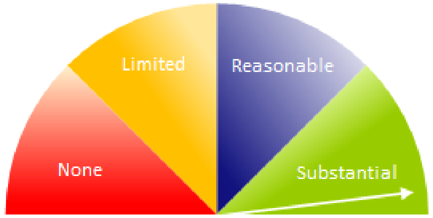
In the Incident Management Audit report, we noted that significant cyber related security incidents are widely considered to be a matter of 'when', not 'if'. A major part of an organisation's first line of defence against attempted cyber-attacks includes a satisfactorily deployed anti-malware solution across a networked estate of connected devices, combined with end-user cyber-security awareness training. It is noted that whilst new starters are subject to mandatory awareness training, the existing end-user base has not received full refresh awareness training for an extended period of time. We note the published training calendar has security awareness training planned for Quarter 4 2022, however, due to the lengthy period of time without it, coupled with current prolonged periods of remote working, bringing forward this training should be considered as part of the security strategy.

Business Grant Post Payment Assurance – Final Audit Report – May 2021

Audit Objective

To provide assurance that COVID-19 related business grants were paid to eligible businesses, in accordance with Government guidance.

Assurance Opinion



A sound system of governance, risk management and control exists, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.

Number of Actions

Priority	Number
Priority 1	0
Priority 2	0
Priority 3	0
Total	**0**

Risks Reviewed	Assessment
If sufficient checks and controls are not in place, ineligible recipients may receive COVID-19 business grants resulting in potential financial, fraud and reputational risk to the Council.	Low

Key Findings

In April 2020, the first round of COVID-19 support grant payments was made to business rate payers within the district. The information on grant applications was checked against the information already held within Civica prior to payment being made.

We have recently undertaken post payment assurance checks and can confirm that no significant findings were made as a result of this work. All COVID-19 business grants tested were found to have been paid to eligible businesses, in accordance with Government guidance.

We can confirm post payment checks have been and continue to be undertaken by the Counter Fraud Team to identify potential fraudulent claims and then subsequent recovery actions where required. We have taken this assurance as well as the post payment assurance checks we have undertaken to support our overall opinion.

Audit Scope

A review of a sample of high value (£10,000 - £25,000) COVID-19 business grants payments made during April 2020, was carried out to ensure that the payments were made to eligible recipients, in line with Government guidance.

Conclusion

We conclude that robust and effective processes have been developed in a short space of time to ensure that grants are paid to qualifying businesses in these trying times. Where fraudulent claims are identified, processes are in place to recover the funds.