

WEST OXFORDSHIRE DISTRICT COUNCIL
AUDIT AND GENERAL PURPOSES COMMITTEE:
THURSDAY 8 NOVEMBER 2018
INTERNAL AUDIT PROGRESS REPORT
REPORT OF THE CHIEF FINANCE OFFICER
(Contact: Jenny Poole Tel: (01285) 623313)

1. PURPOSE

To consider the key findings of recent internal audits and provide an update regarding progress against the internal audit plan for 2018/19.

2. RECOMMENDATION

That the report be noted.

3. BACKGROUND

- 3.1. The Internal Audit Service is delivered by South West Audit Partnership (SWAP) Internal Audit Services, which is a local authority owned company.
- 3.2. This report sets out the work undertaken by SWAP since the Committee's last meeting. It follows the risk-based auditing principles and, therefore, presents an opportunity for the Committee to be aware of emerging issues which have resulted in SWAP involvement.
- 3.3. Progress against the 2018/19 Audit Plan, which was approved by this Committee in April 2018, is included in the SWAP Report of Internal Audit Activity Plan Progress in the [Appendix](#).
- 3.4. Copies of the full reports, which include terms of reference, detailed findings and recommendations for improvement specifying target dates and the officers responsible for implementation, are available for members on request.

4. ALTERNATIVES/OPTIONS

Not applicable.

5. FINANCIAL IMPLICATIONS

This report has no direct financial implications. The audits were carried out in accordance with the agreed audit plans and budgets for 2018/19.

6. REASONS

The report is presented pursuant to the Committee's role in monitoring the audit function for the Council.

Lucy Cater
Assistant Director, SWAP Internal Audit Services

(Author: Lucy Cater, Tel: (01285) 623340; Email: lucy.cater@swapaudit.co.uk)

Date: 24 October 2018

Background Papers:
None



West Oxfordshire District Council

Report of Internal Audit Activity

Plan Progress 2018/2019

November 2018

Contents

The contacts at SWAP in connection with this report are:

Gerry Cox

Chief Executive

Tel: 01935 385906

gerry.cox@swapaudit.co.uk

Ian Baker

Director of Quality

Tel: 07917628774

ian.baker@swapaudit.co.uk

Lucy Cater

Assistant Director

Tel: 01285 623340

lucy.cater@swapaudit.co.uk

●	Role of Internal Audit	Page 1
●	Internal Audit Work	Page 2
●	Approved Changes to the Audit Plan	Page 3
●	Appendices:	
	Appendix A – Internal Audit Definitions	Page 4 – 5
	Appendix B – Internal Audit Work Plan Progress	Page 6 – 10
	Appendix C – Executive Summary of Finalised Audit Assignments	Page 11 – 18
	Appendix D – High Priority Recommendation Follow-Up	Page 19 – 25
	Appendix E – Summary of All Recommendations	Page 26 – 27

Internal Audit Plan Progress 2018/2019

Our audit activity is split between:

- **Governance Audit**
- **Operational Audit**
- **Key Control Audit**
- **IT Audit**
- **Other Reviews**

● Role of Internal Audit

The Internal Audit service for West Oxfordshire District Council is provided by SWAP Internal Audit Services (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.

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

- Governance Audits
- Operational Audits
- Key Financial System Controls
- IT Audits
- Other Special or Unplanned Review

Internal Audit work is largely driven by an Annual Audit Plan. This is recommended to the Audit and General Purposes Committee by the Chief Finance Officer, following consultation with the Council's Management Team. The 2018/19 Audit Plan was reported to, and approved by, Audit and General Purposes Committee at its meeting in April 2018.

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

Internal Audit Plan Progress 2018/2019

Outturn to Date:

We rank our recommendations on a scale of 1 to 3, with 1 being a major area of concern requiring immediate corrective action and 3 being a minor or administrative concern

● Internal Audit Work

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** of this document.

The schedule provided at **Appendix B** contains a list of all audits as agreed in the Internal Audit Annual Plan 2018/19. 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.

As is shown in **Appendix B** progress is being made on the 2018/19 audit plan, following the completion of the 2017/18 plan.

As agreed with this Committee where a review has a status of ‘Final’ we will provide a summary of the work and further details to inform Members of any key issues, if any, identified.

Further information on all the finalised reviews can be found within **Appendix C**.

At **Appendix D** we have included a schedule of the high priority recommendations that were identified during 2017/18. These will be updated when the follow-up audit has been completed.

Internal Audit Plan Progress 2018/2019

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

- Approved Changes to the Audit Plan

The audit plan for 2018/19 is detailed in **Appendix B**. Inevitably changes to the plan will be required during the year to reflect changing risks and ensure the audit plan remains relevant to West Oxfordshire District Council. Members will note that where necessary any changes to the plan throughout the year will have been subject to agreement with the appropriate Service Manager and the Audit Client Officer.

We are undertaking an audit of Disabled Facilities Grants, following a request from the Service Manager. This was agreed with the Chief Finance Officer and days have been taken from contingency.

We have also taken 2 days from contingency to allow for a follow-up review to be undertaken for Private Water Supplies.

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

- **No Assurance**
- **Partial**
- **Reasonable**
- **Substantial**

Audit Framework Definitions

Control Assurance Definitions

No 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.
Partial	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.
Reasonable	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.
Substantial	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.

Non-Opinion – In addition to our opinion-based work we will provide consultancy services. The “advice” offered by Internal Audit in its consultancy role may include risk analysis and evaluation, developing potential solutions to problems and providing controls assurance. Consultancy services from Internal Audit offer management the added benefit of being delivered by people with a good understanding of the overall risk, control and governance concerns and priorities of the organisation.

Recommendations are prioritised from 1 to 3 on how important they are to the service/area audited. These are not necessarily how important they are to the organisation at a corporate level.

Each audit covers key risks. For each audit a risk assessment is undertaken whereby with management risks for the review are assessed at the Corporate inherent level (the risk of exposure with no controls in place) and then once the audit is complete the Auditors assessment of the risk exposure at Corporate level after the control environment has been tested. All assessments are made against the risk appetite agreed by the SWAP Management Board.

Audit Framework Definitions

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.

	Categorisation of Recommendations
Priority 1	Findings that are fundamental to the integrity of the service's business processes and require the immediate attention of management.
Priority 2	Important findings that need to be resolved by management
Priority 3	Finding that requires attention.

Definitions of Risk

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

Audit Type	Audit Area	Quarter	Status	Opinion	No of Rec	5 = Major		↔	1 = Minor		Comments
						Recommendation					
						5	4	3	2	1	
2017/18 Audits – Draft / In Progress at Annual Opinion											
ICT	Protection from Malicious Code		Position Statement								
ICT	ICT Policies		Final Report	Reasonable	1			1			See Appendix C
ICT	Public Services Network Submission (PSN)		Final Report	Reasonable	2			2			See Appendix C
Key Financial Control	Fighting Fraud Locally		Final Report	Reasonable	5		1	4			See Appendix C
Key Financial Control	Serious and Organised Crime Checklist		Final Report	Reasonable	1			1			See Appendix C
Key Financial Control	Serious and Organised Crime Audit										

Internal Audit Work Plan Progress 2018/2019

APPENDIX B

Audit Type	Audit Area	Quarter	Status	Opinion	No of Rec	Priority			Comments
						1	2	3	
2018/19 Audit Plan									
Governance	Annual Governance Statement	1	Final Report	Substantial	-				See Appendix C
ICT	Data Protection Act 2018 (GDPR)	1	ToR Agreed						Deferred by request of Client in quarter 1, audit re-commenced
Operational	Procurement and Contract Management	1	ToR Drafted						Deferred by request of Client to quarter 3 / 4. Audit Re-commenced
Operational	Refugees	1	Draft Report						
Operational	Disabled Facilities Grants (NEW)	1	Draft Report						
Other Audit Involvement	Disabled Facilities Grant Certification	1	Complete	N/A					
Governance	Performance Management	2	In Progress						
ICT	Public Services Network Submission (PSN)	2							
Operational	Members and Officers Gifts and Hospitality and Declarations of Interest	2	In Progress						
Operational	Regulatory Awareness and Compliance	2	In Progress						
Operational	Internal Enforcement Agency	2	Draft Report						

Internal Audit Work Plan Progress 2018/2019

APPENDIX B

Audit Type	Audit Area	Quarter	Status	Opinion	No of Rec	Priority			Comments
						1	2	3	
Operational	S106 Agreements and Funds	2	In Progress						
Operational	Subsidy Claims	2	Deferred						Deferred by request of Client to quarter 3 / 4
Follow-Up	Licensing	2	Draft Report						
Follow-Up	Food Safety	2	Draft Report						
Follow-Up	Security	2	Draft Report						
Follow-Up	Safeguarding	2	In Progress						
Follow-Up	Pool Cars	2	Final Report						
Key Financial Control	Revenues and Benefits	3	ToR Agreed						
	• National Non-Domestic Rates								
	• Council Tax								
	• Council Tax Benefit								
Key Financial Control	Core Financials	3	Scope Drafted						
	• Accounts Payable								
	• Accounts Receivable								

Audit Type	Audit Area	Quarter	Status	Opinion	No of Rec	Priority			Comments
						1	2	3	
	• Main Accounting								
	• Payroll								
	• Treasury Management and Bank Reconciliation								
Key Financial Control	Systems Administration	3							
Key Financial Control	Human Resources	3							
Key Financial Control	Other Support Service provided by Publica • Procurement	3							
Governance	Risk Management	4							
Key Financial Control	Serious and Organised Crime	4							
Operational	Corporate Culture	4							
Operational	Discretionary Housing Payments	4	Draft Report						
Follow-Up	Private Water Supplies (NEW)	4							
Follow-Up Audits	Follow-Ups of Recommendations made in Substantial and Reasonable Audits	1 – 4	On Going						

Internal Audit Work Plan Progress 2018/2019

APPENDIX B

Audit Type	Audit Area	Quarter	Status	Opinion	No of Rec	Priority			Comments
						1	2	3	
	• Public Health Burials		Complete						See Appendix E
	• Health and Safety		Complete						See Appendix E
	• Public Services Network (PSN)		Complete						See Appendix E
	• ICT Policies		Complete						See Appendix E
	• Grant Payments to Third Parties		In Progress						
	• IR 35		In Progress						
Advice and Consultancy	Benefits Realisation	1 - 4							
Advice and Consultancy	Public Governance	1 – 4	On Going						
Advice and Consultancy	Change Programmes (Public Transformation Programme)	1 – 4	On Going						
Other Audit Involvement	Provision for Grant Certifications	1 – 4							
Other Audit Involvement	Management of the IA Function and Client Support	1 – 4	On Going						
Other Audit Involvement	Contingency – Provision for New Work based on emerging risks								

Audit Type	Audit Area	Quarter	Status	Opinion	No of Rec	Priority			Comments
						1	2	3	
	Other ICT Audits – to be agreed with SWAP ICT Auditor and ICT								

Audit Assignments finalised since the last Audit Committee:

Summary of Audit Assignments Finalised since the last Audit Committee

● **Summary of Audit Findings and High Priority Service Findings**

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

2017/18 Protection from Malicious Code – Position Statement

We were unable to complete all sufficient system control testing in order to provide an audit opinion at this time due to the availability of key staff, however we have assessed the residual risk and provided this position statement based on the strategic approach and systems that Publica have in place to protect the Council's network, systems and data from the effects of viruses and malicious code.

We have also based our findings on recent audit reviews of the independent IT Health Checks (ITHC) and PSN submission activities, and our review of ICT Policies (Data backup and Ransomware Policies). here were no significant issues and we noted that progress has been made against the independent ITHC, internal audit, and Publica - IT's own findings.

Initiatives were underway to improve the security of the Council's network and Partner data using the latest intelligent threat protection products.

All high-risk vulnerabilities to Council systems, including those arising from a number of unsupported systems have been resolved, and key corporate systems had either been updated with the latest software, or software updates were being tested prior to deployment.

The Patch Management and, Change Control Policies, have been revised and updated. The Information Security Standards Policy has also been revised and updated to provide consistent direction and guidance to users across all Council Partners. As at March 2018, Publica – IT were also in the process of creating a Cloud Computing Policy, to better inform their clients as to the risks from future use of open system providers, and to govern the use of this technology.

The PSN Authority have issued Publica with new annual certificates, that commenced in May 2018, for each of the four Councils.

There were several well controlled areas, and whilst we consider that there are sufficient controls to avoid a high impact attack, and it is likely that attacks will be confined to a user's computer and file shares, there will always be a risk from a virus infection, as those who target find more ways to cheat defences, and anti-virus products.

Therefore, we have assessed that there is a Medium residual risk.

2017/18 Public Services Network Submission – Reasonable Assurance

Our findings are based on reviewing the PSN activities, the PSN submission timeline, and meetings held with the Chief Technology Officer and the ICT Audit and Compliance Manager.

We are able to provide a reasonable audit opinion on the status of submission of the annual PSN Commitment Statement (Code of Connection) and supporting documentation.

The IT External and Internal Health Checks (ITHC) were carried out in November 2017, identified no critical or serious vulnerabilities and neither did they raise any high vulnerabilities during external penetration testing, which demonstrated that the Council's network was designed to a sufficient standard to mitigate the known risks of being attacked from an outside source. Only medium and Low risk vulnerabilities were found during external testing, these include weak ciphers, web server issues and weak transforms.

High risk vulnerabilities were only discovered on the internal network after the Chief Technology Officer provided independent penetration testers with passwords, upon request from the testers. This identified client software, which was unsupported, and therefore could not be updated to bring the software security up to current standards. Publica IT then proceeded to work with their clients to remove those vulnerabilities, which caused a delay in the original submission.

At the time of our initial review, in February 2018, not all actions arising from the independent Internal and External IT Health checks had been completed. However, it should be noted that there was a short timeframe between the findings of the testing being reported and the internal audit review.

The compliance statement and supporting documentation was initially submitted to the Cabinet Office on 8 January 2018, after being signed off by the Senior Officer at each Partner Authority, prior to the certificate expiring on 19 January 2018. This submission was accepted by the PSN Authority with the caveat that the actions to address the high vulnerability areas were carried out by the 31 March 2018, and for an updated Remediation Action Plan to be resubmitted to PSN A.

There were originally 36 high risk vulnerabilities raised, on the ITHC, and at the time of resubmission, on 23 March 2018, only 1 high risk vulnerability was outstanding. In the period, whilst addressing the actions, there had been liaison between Publica IT and the PSN team at the Cabinet Office to inform them of the progress.

At the time of writing this report, PSN A have now validated the re-submission from Publica IT and have passed it to their assessors before issuing a new PSN certificate.

Out of the 47 medium and low risk issues, raised on the ITHC, 18 actions remained open, and 29 actions had been reported closed. Out of the 29 closed risks, there were thirteen low risk vulnerabilities that had been risk assessed and accepted by the Chief Technology Officer, rather than having actions assigned to them.

Addressing these vulnerabilities was being carried out with the background of 'Meltdown' and 'Spectre' vulnerabilities which have arisen from the flawed design of the commonly used processor chip and highlighted on 3 January 2018 as a World issue. This will mean software / firmware upgrades and engineering visits, by Publica IT, to desks and all IT equipment rooms to make configuration changes to the Bios on computer equipment.

We concluded that all mandatory documentation had been submitted to the PSN A and that care had been taken in ensuring that only accurate information had been entered onto the PSN Commitment Statement. The results from the Internal and External ICT Health Checks had been accurately transferred onto Remediation Action Plan.

We took assurance on the effectiveness of the design of the security controls from the independent Internal and External ICT Health checks that had recently been commissioned, the response to the security risks that had been identified, and a review of a sample of the joint information security policies, risk registers, and interviews with key staff.

There were four security gaps detailed in the PSN Commitment Statement. Resource had been made available to address these gaps in compliance. One of the 4 gaps identified, 'Cloud computing', represented no current risk, as this technology was not used, however a Cloud computing policy is being drafted, so that the Partnership is ready for future considerations of this technology and have an understanding to the risks open to system providers.

ICT Operations Patch Management Policy, headed with CDC, FODDC and WODC logos and updated by Publica in August 2017, needed updating to include CBC and make it explicit how networked, unsupported systems will be treated by Publica IT, and the Policy needed an understanding and approval from each of the 4 Councils.

We found that risks were assessed and communicated across service and corporate risk registers, and that mitigating controls listed on those registers were monitored and evidenced. We have, however, made two Priority 3 recommendations, that when implemented will further improve the risk control framework.

2017/18 – ICT Policies – Reasonable Assurance

As part of the agreed 2017-18 Internal Audit Plan a review has been undertaken to assess the adequacy and effectiveness of ICT Policies across the Partnership. It is important where a shared service is being delivered to a number of partners that users from each authority abide by common policies to ensure consistent security behaviour across the Partnership's network.

There have been a number of high-profile cases where public sector organisations, including Councils, have been targeted with 'ransomware' viruses.

The term 'Ransomware' describes a form of virus which can lock up data stored on Council systems, which can only be unlocked upon payment of a ransom. There is a risk that if users adopt the wrong behaviour, it can inadvertently allow malicious code to traverse the Council's network and encrypt it. This could be because of poorly documented user responsibilities.

The protection of ransomware is part of the suite of controls in place to prevent threats from viruses, and malicious code.

If reliable backups of data are held, data can be restored, and the corrupted data destroyed. Therefore, policies relating to anti-virus and data backup are important components in the ICT set of policies.

The purpose of this piece of work is to review the ICT Policies used by each authority to provide assurance that ICT Data backup and Ransomware Policies address risk, are consistently implemented across the Partnership, and are controlled and accessible to all users.

Audit testing took place in February 2018 and all findings contained within this report were correct at the time of testing. Since completion of the fieldwork Cheltenham Borough Council (CBC) have adopted the new shared Information Security Policy along with Cotswold District Council (CDC), Forest of Dean District Council (FoDDC) and West Oxfordshire District Council (WODC). CBC now has access to the same suite of improved control documentation and has aligned itself with the other partner councils.

2017/18 – Serious and Organised Crime – Reasonable Assurance

The Serious and Organised Crime Strategy (2013) was introduced by the government and confirms;

"There is no legal definition of organised crime in England and Wales. For the purposes of this strategy, organised crime is serious crime planned, coordinated and conducted by people working together on a continuing basis. Their motivation is often, but not always, financial gain."

The Strategy estimates there were roughly 5,500 active Organised Crime Group's (OCG) in the UK at the time who were responsible for;

- The trafficking of drugs, people and firearms
- Organised illegal immigration
- Large-scale and high-volume fraud and other financial crimes
- Counterfeit goods (including medicines)
- Organised acquisitive crime
- Cyber crime

Since the Strategy was implemented, the Counter Fraud Unit (CFU) was established across Gloucestershire and West Oxfordshire (April 2017) and this Council has appointed them to provide assurance over its counter fraud measures. Meeting minutes support the CFU report bi-annually to Members, and the CFU's Counter Fraud and Anti-Corruption Policy (2017) and Whistleblowing Policy (2016) have been approved and adopted.

The 'Serious and Organised Crime Checklist Self-assessment' has been completed by the CFU and has identified areas where controls should be in place, and areas which they acknowledge need improvement.

The Council is a member of the National Fraud Initiative (NFI) and Counter Fraud data is published on its website annually. The CFU Manager and Internal Audit Assistant Director meet quarterly to discuss any areas of concern and an annual meeting is held with the Councils External Audit provider. CFU staff all have previous experience in relevant areas of the Public Sector and have good links and to relevant external organisations. The CFU Manager is also the serious and organised crime single point of contact for the region and they have quarterly meetings in relation to this role which also provides good links for intelligence sharing.

Risk Management and Procurement processes in relation to serious and organised crime have been identified as areas requiring improvement and we would agree with this assessment; further work will be undertaken to provide assurance over these practices in 2018/19. The CFU have also stated that controls in relation to licensing and planning are currently due to be followed up, so we have been unable to provide an assessment in these areas.

Working with the CFU should help the Council keep up to date with current threats, so any vulnerabilities can be identified and mitigated against as much as is possible. By appointing the CFU the Council is demonstrating it has implemented measures to try and tackle Serious and Organised Crime in accordance with the government's strategy, which should also feed into helping the Council to achieve its aim/vision by acknowledging and understanding its risks.

2017/18 – Fighting Fraud and Corruption – Reasonable Assurance

We have reviewed the current arrangements in place to combat fraud and corruption across West Oxfordshire District Council (WODC). The 'Fighting Fraud Locally Checklist' has been completed to assess operations in relation to the three core principles of the Local Government Counter Fraud and Corruption Strategy (2016-2019): Acknowledge, Prevent and Pursue.

The Counter Fraud Unit (CFU) was established across Gloucestershire and West Oxfordshire in April 2017, and WODC have appointed them to provide assurance over their counter fraud practices. The Counter-Fraud & Anti-Corruption Policy (2017) has been shared with WODC Members for their consideration and it is available on the Council website; meeting minutes support Members have approved this policy. The following documentation is also in place at the Council to help communicate its approach to fraud and provide guidance for Members and Officers;

- Council Constitution • Member Code of Conduct • Officer Code of Conduct • Whistleblowing Policy

Going forward, we would suggest the CFU and Internal Audit are consulted when reviewing the Constitution, Member and Officer Codes of Conduct and Council policies in areas where potential fraud may occur, to ensure current fraud and risk themes are considered and guidance reflects this. The Council has a Corporate Risk Register in place, but fraud risks are not easily identifiable; this has been flagged as an area of improvement by the CFU and we would agree with this assessment.

An Annual Governance Statement (AGS) is documented and shared with Audit and General Purposes Committee. Any risks identified in the AGS are followed up in line with the annual audit plan; the CFU are also consulted on the drafting of the annual Internal Audit plan.

At the time of audit work, CFU Awareness training was delivered to Council Staff and it was confirmed the training slides would be added to the Publica Portal for Officer information. We would suggest the current Counter-Fraud & Anti-Corruption Policy is also added to the Publica Portal to ensure Officers can easily access the guidance; the CFU Manager confirmed this has been requested. Members should be directed to the CFU webpage on the Council's website to access the policy.

The Council takes part in the National Fraud Initiative (NFI) and publishes Counter Fraud data on its website annually. CFU staff have relevant experience within the Public sector to undertake the work included within the annual plan and can work with other agencies when necessary to ensure professionally trained staff undertake work.

Member registers of interest and gifts can be requested from the Council, but they are not published on its website. The Council's Procurement Strategy is now outdated and needs to be reviewed. Further reviews of procurement and registers will be undertaken by the CFU and Internal Audit in their 2018/19 work plans. BPSS (Baseline Personnel Security Standard) checks should be undertaken on all Council staff however the CFU have identified that this is also an area which will be reviewed further in the 2018/19 work plan. The Council should also ensure Publica staff delivering its services have the appropriate checks in place.

Our review has found controls are in place to help the Council fight fraud locally, and the improvements suggested within this report will help to strengthen what has already been implemented. Ensuring controls are consistently adhered to across the CFU's partners will provide a joined-up approach across the local area and help all partners acknowledge, prevent and pursue fraud in line with government guidance.

2018/19 – Annual Governance Statement – Substantial Assurance

The Heads of Service and Directors were asked to complete and return a Management Assurance Statement (MAS). The MAS is a declaration that adequate governance measures are in place.

A proportion of the managers assurance statements were examined and were confirmed as completed fully and correctly and in line with the required templates. The MAS are therefore able to be taken as assurance in compiling the Annual Governance statement.

The Annual Governance statement was compared to the CIPFA Governance Framework (2016) and was completed in line with the framework's requirements. The statement was drafted, discussed and considered at the Audit and General Purposes Committee meetings ahead of the deadline of 31st May. The statement is publicly available within the Annual Statement of Accounts on West Oxfordshire District Council's website.

It is recognised that the Annual Governance statement is drafted by the Head of Internal Audit based on MAS returns and knowledge of the governance environment gained through audit work carried out during the year. It should be noted that although requested by the Council, consideration should be given to it being completed outside of internal audit to further demonstrate independent assessment.

High Priority Recommendation Follow-Up

APPENDIX D

Audit Name	Priority	Recommendation	Management Response	Due Date	Update October 2018
2017/18 – Food Safety	1	<p>"The Service Business Manager, has agreed to ensure that: -</p> <ul style="list-style-type: none"> • the document, Delegated powers to officers of the Environmental and Regulatory Services group, is signed off at the appropriate level for all officers whose duties are detailed within it. • Officers individually have written authorisation to carry out duties under the Food Safety and Hygiene (England) Regulations 2013 and the Official Feed and Food Controls (England) Regulations 2009. • Clarification is sought from Legal to confirm Publica officers have the legal authorisation to carry out all their duties relating to food business premises on behalf of the Councils" 	<p>Delegated powers to officers of the Environmental and Regulatory Services group will be signed off.,</p> <ul style="list-style-type: none"> • Individual Officers now have written authorisation to carry out duties under the Food Safety and Hygiene (England) Regulations 2013 and the Official Feed and Food Controls (England) Regulations 2009 • All managers now have dual contracts outlining legal authorisations, however further clarification around some issues is ongoing." 	31/05/18	<p>Follow-Up Audit Complete Recommendation Complete</p> <p>Officers now have delegated powers by virtue of individual documents authorised by the ERS Food Safety Service Leader. Signed copies of these documents have been uploaded and saved within the services shared files.</p> <p>The Service Leader has a shared contract of employment between Publica and the partner Councils (Cotswold, Forest of Dean and West Oxfordshire). This contract states the Service Leader has delegated functions under a number of Acts and Regulations that allow her to fully carry out her role.</p> <p>The service has consulted with the Councils' legal services to ensure ERS officers hold the appropriate authorisations to carry out their duties on behalf of the Councils. This has been verified with Legal as part of this review.</p>

High Priority Recommendations

APPENDIX D

Audit Name	Priority	Recommendation	Management Response	Due Date	Update October 2018
2017/18 – Food Safety	2	The Lead Officer has agreed to ensure inspections are carried out in accordance with the Food Law Code of Practice intervention frequencies to comply with its statutory duties to enforce legislation relating to food.	<p>The FSA are currently reviewing the timescale (28 days) in which due inspections must be made as local authorities nationally are struggling to achieve this. ERS will aim to prioritise inspections according to risk and where able inspect within 28 days of the due date.</p> <p>Overdue inspections are monitored at monthly team Meetings."</p>	28/02/18	<p>Follow-Up Audit Complete Recommendation in Progress</p> <p>As outlined in our food service plans we will commit to ensure A's, B's and non-compliant C's are delivered within 28 days, thus employing a risk-based approach in accordance with the Framework Agreement on Local Authority Food Law Enforcement.</p> <p>Revised Implementation Date 31/10/18</p>
2017/18 – Licensing	2	We recommend that the requirements of licensing enforcement operations are documented. The activities that are carried out during the operations should also be documented to provide evidence and support any resulting actions that are taken by officers.	As a result of this review, some training needs and opportunity for process improvement have been highlighted. A Licensing team training session will be held on how to record this pro-active enforcement work, and in relation to the use and closure of service requests on Uniform for enforcement related actions."	31/08/18	<p>Follow-Up Audit Commenced Recommendation in Progress</p> <p>Pro-Active enforcement action was carried out in August, Licensing Officer waiting for feedback from parties involved, prior to making amendments to process and drafting</p> <p>Revised Implementation date 31/10/18</p>

High Priority Recommendations

APPENDIX D

Audit Name	Priority	Recommendation	Management Response	Due Date	Update October 2018
2017/18 – Licensing	2	We recommend that the procedure for debt recovery for premises and club premises licences is amended to be in accordance with relevant legislation.	In accordance with the legislation the current procedure for debt recovery will be amended to ensure that Premises and Club Licences are suspended after 21 days of an invoice becoming due. ERS will request the assistance of Accounts Receivable to assist with this task.	31/08/18	Follow-Up Audit Commenced Recommendation in progress Revised Implementation date 31/10/18
2017/18 – Other GOSS Area Health and Safety	2	GOSS HS should produce a list of duties carried out at each of its clients and document any associated risks. Appropriate policies should then be written on behalf of each client and approved at the appropriate level.	HS policies are already in place at CBC, CDC, FoDDC, Ubico and WODC. These will continue to be reviewed in line with current procedures. The working practices of officers transferring into Publica aren't due to change significantly, therefore existing Council HS policies will be branded for Publica use and approved by the Board. In the interim period until Publica Board can meet to approve these policies, the GOSS HS Manager (in his role as advisor to Publica) has produced a transformation document stating there will be a brief transition period, until all policies have been adopted by Publica, which all Publica employees will be required to comply with Council policies."	30/03/18	Follow-Up Audit Complete Recommendation Complete All HS policies currently still in place for CBC, CDC, FODDC and WODC. Publica adopted a more streamlined approach, retaining a Corporate H&S Policy supported by more user-friendly statements and guidance documents rather than a vast number of policies which may not be relevant to everyone in the organisation. All documents ready to go on the portal. (just waiting for final approval) Same approach will be taken for council retained staff

High Priority Recommendations

APPENDIX D

Audit Name	Priority	Recommendation	Management Response	Due Date	Update October 2018
2017/18 – Other GOSS Area Health and Safety	2	The GOSS HS Manager should work with senior management from each of GOSS's clients to ensure each appoints a 'responsible person' in line with the Regulatory Reform (Fire Safety) Order 2005. This should be a senior officer who is made aware of all responsibilities that come with the position.	OSS HS, in consultation with their clients, have identified Responsible Persons at each client (including Publica). Training on the role and responsibilities of the position will be provided to each officer at which time appointment letters will be issued."	31/01/18	Follow-Up Audit Complete Recommendation Complete Responsible persons under "the regulatory reform (fire safety) order 2005": CDC: Nigel Adams WODC: Giles Hughes FODDC: Peter Williams (All trained in July 2018)
2017/18 – IR35	2	To ensure compliance with HMRC guidance, all supplier request forms should be updated to state the service manager from the hiring authority is responsible for completing the ESS to determine employment status.	Revise the new supplier request form to reflect the responsibilities on the public body not sole trader.	31/07/18	Follow-Up Audit Complete Recommendation Complete Amendments to the form have been made and checked by the relevant teams.
2017/18 – IR35	2	An individual / service area should be assigned to oversee and own the IR35 process to ensure accountability.	Each Group Manager should appoint a person responsible for Overseeing the IR35 process and maintaining a register of 'off payroll' workers to avoid delays with recruiting.	31/07/18	Follow-Up Audit Complete Recommendation Complete A register has been created and all Group Managers have been given access to this as well as relevant information / guidance.

High Priority Recommendations

APPENDIX D

Audit Name	Priority	Recommendation	Management Response	Due Date	Update October 2018
2017/18 - Safeguarding	2	A process should be put in place to ensure that the Safeguarding Policy is embedded into all contracted services or to ensure that contractors have a sufficient regard for Safeguarding which is equivalent to the requirements of the authority's Safeguarding Policy. This process should include a method of gaining continued assurance that a supplier is abiding by the Safeguarding requirements of the Council.	This is a matter that can be discussed with the procurement team. It will also need to be part of discussions as part of the new contractual arrangements between CDC and Publica."	01/04/18	Follow-Up Audit Commenced
2017/18 - Safeguarding	2	"The 'Lead Designated Safeguarding Officer', who is accountable for the effective delivery of the Safeguarding Policy, must obtain assurance that the training requirements of the policy are met. In order to gain such assurance, it is recommended that a full review of the approach to training is undertaken for all 'employees' and Members. Focus should be given to the following: - The introduction of Safeguarding into the Corporate Induction process - Development of a plan for Safeguarding training for staff and Members and to include a timeframe for completing the training requirements - Introduction of a method of recording staff training and understanding of training content"	The LSO, together with the Community Safety Officer, now attend induction sessions to give a presentation in respect of safeguarding and PREVENT. A training plan/strategy is being developed that will outline training requirements for staff and councillors and how this will be delivered. Safeguarding of children and vulnerable adults is now included on the new online training system and other courses will be added as appropriate. Details of completion of the courses will be recorded on the system."	31/12/17	Follow-Up Audit Commenced
2017/18 – Accounts Payable (Creditors)	2	The Accounts Payable Accountancy Manager should ensure that a quarterly review of all payments made during the past four months is undertaken to highlight any duplicate payments made.	We will run this new process for the middle of each quarter, i.e. February, May, etc. This will allow us time to make any necessary adjustments before quarter end.	01/06/18	Will be followed-up during core financial audit in quarter 3

High Priority Recommendations

APPENDIX D

Audit Name	Priority	Recommendation	Management Response	Due Date	Update October 2018
2017/18 – Fighting Fraud and Corruption	2	The CFU should be consulted when the Procurement and Contract Strategy is reviewed to ensure fraud in relation to procurement is fully considered.	CFU Manager to work with Procurement and assist with a revised Strategy"	23/07/18	Will be followed-up during Serious and Organised Crime Audit in quarter 4

Summary of Recommendations made in 2017/18 Internal Audit Reports					
Audit	Assurance Score	Total	Recommendations		
			Complete	In Progress	*Not Due / F/Up in Progress
Equalities and Diversity	Reasonable	2			2
Public Health Burials	Substantial	4	4		
Health and Safety	Reasonable	2	2		
Licensing	Reasonable	11	6	5	
Food Safety	Partial	8	4	4	
Accounts Payable	Reasonable	1	1		
Payroll	Substantial	2			2
Accounts Receivable	Reasonable	2			2
Risk Management	Partial	5			5
Business World Systems Admin	Reasonable	2	1	1	
Main Accounting	Substantial	1	1		
IR35	Reasonable	5	2		3
Safeguarding	Partial	6			6
Grant Payments to Third Parties	Reasonable	2			2
ICT Policies	Reasonable	1	1		
Public Services Network	Reasonable	2	2		
Fighting Fraud Locally	Reasonable	5			5
Serious and Organised Crime	Reasonable	1			1
		62	24	10	28
*Not Due - will be followed up during core audits, Follow-up audit is in progress or the implementation date has not been reached					



