

West Oxfordshire District Council

Report of Internal Audit Activity

January 2025

Contents

The contacts at SWAP in connection with this report are:

Lucy Cater

Assistant Director

Tel: 01285 623340

lucy.cater@swapaudit.co.uk

Jaina Mistry

Principal Auditor

Tel: 01285 623337

jaina.mistry@swapaudit.co.uk

- Contents:

Internal Audit Definitions

Audit Plan Progress

Finalised Audit Assignments

Internal Audit Definitions

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

- **No**
- **Limited**
- **Reasonable**
- **Substantial**



Audit Framework Definitions

Control Assurance Definitions

No	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control is inadequate to effectively manage risks to the achievement of objectives in the area audited.
Limited	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
Reasonable	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Substantial	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.

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.

Internal Audit Definitions

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	Status	Opinion	No of Rec	Priority			Comments
					1	2	3	
Operational	Appointment of Consultants	Final Report	Mid Reasonable	2	-	1	1	Reported In September
Operational	Accounts Payable – Qtly Review – 2023/24	Final Report	High Substantial	0	-	-	-	Reported In September
Operational	Emergency Planning	Final Report	Low Substantial	1	-	-	1	Reported in November
Operational	Members Allowances and Expenses	Final Report	Low Reasonable	2	-	2	-	Reported in November
Operational	Levelling Up Funding – UKSPF and RESF	Final Report	Low Substantial	0	-	-	-	Report Included
Governance	Data Protection / Breaches	Final Advisory Report	N/A	0	-	-	-	Report Included
Operational	Human Resources	Final Advisory Report	N/A	4	2	1	1	Report Included
Key Financial Control	Revenues and Benefits – Council Tax and NNDR	Final Report	High Reasonable	2	-	1	1	Report Included
Key Financial Control	Revenues and Benefits – Council Tax Benefit and Housing Benefits	Final Report	Mid Substantial	0	-	-	-	Report Included
Operational	Section 106s	Draft Report						
Follow-Up	Procurement Cards	In Progress						
Follow-Up	Taxi Licensing Safeguarding	In Progress						
Operational	Planning Fee Obligations	In Progress						
Core Financial	Payroll	In Progress						
Operational	CFEU	In Progress						

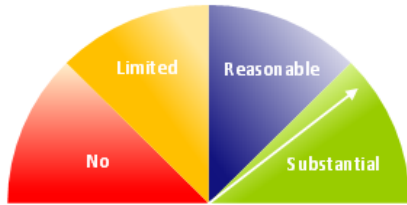
Audit Type	Audit Area	Status	Opinion	No of Rec	Priority			Comments
					1	2	3	
Advisory	Procurement and Commissioning Group	On-Going						
Advisory	Health and Safety Working Group	On-Going						
Advisory	Corporate Governance Group	On-Going						
Support	Co-Ordination Team / Emergency Planning	On-Going						
Follow-Up	Follow-Up of Agreed Actions (not included in an audit above)	On Going						
Other Audit Involvement	Working with the Counter Fraud and Enforcement Unit	On Going						
Other Audit Involvement	Management of the IA Function and Client Support	On Going						
Other Audit Involvement	Contingency – Provision for New Work based on emerging risks							

Levelling Up Funding (UKSPF and REPF) – Final Report – December 2024

Audit Objective

To provide assurance that Publica has processes in place that ensure proper administration of financial affairs relating to the UKSPF and REPF allocation awarded to West Oxfordshire District Council.

Executive Summary



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.

Management Actions

Priority 1	-
Priority 2	-
Priority 3	-
Total	-

Organisational Risk Assessment

Medium

Our audit work includes areas that we consider have a medium organisational risk and potential impact.

Key Conclusions



We found incomplete records relating to initial UKSPF allocations, dating back to 2022, making it difficult to provide assurance on controls around the initial allocation and selection process, the OxLEP project which is now subject to a renegotiation and downsizing of target outputs and outcomes, being an example. However, no formal recommendation has been made as the officers involved in the project at its inception have now left the authority.



One project was identified (Community Infrastructure Fund) where there remains a possibility of the allocation not being fully utilised. However, we have received assurances that this will not be the case and that contingencies are in place.



There was ample evidence of robust monitoring and pro-active management of projects e.g. the possible renegotiation with OxLEP and contingency plan for the Community Infrastructure Fund project. Financial controls were found to be working well and statutory and internal reporting was timely and comprehensive. Allocations tested were compliant with Central Government UKSPF & REPF guidance.

Audit Scope

We reviewed the following processes:

- The process for allocating UKSPF and REPF funding, including approval of applications and decision-making processes at the Panel.
- The controls in place for making payments, including the checks made to ensure funds have been spent in accordance with the Investment Plan and UKSPF/REPF conditions.
- Processes in place to monitor expenditure.
- Management oversight of the administration of the fund.

The audit covered the period from April 2022 – present.

Other Relevant Information

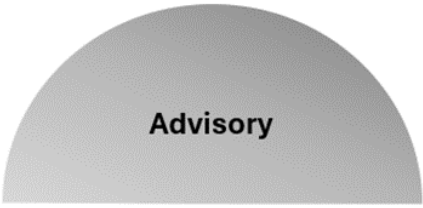
During the audit, SWAP were made aware of a possible conflict of interest involving a WODC Member who is also on the board of OxLEP and a member of the Local Partnership Group. This was outside the scope of this audit but was followed up and has been resolved satisfactorily.

The new government have announced that the UKSPF initiative is being extended into 2025/26. This may mean that existing projects have more time to spend their allocation although this is yet to be confirmed. Officers stated that until this confirmation is forthcoming, their approach will be to continue to regard the existing deadline of 31/3/25 as the cut-off point for spending UKSPF & REPF funding.

Data Protection and Data Breaches – Final Report – November 2024

Audit Objective

An advisory review in respect of Data Protection and the policies and process for Data Breaches.

	Advisory Report	Organisational Risk Assessment	High
	The advice provided in this report encompasses risk analysis and evaluation based on current activity/operations. Please see below for details of why an advisory report has been used.	Our audit work includes areas that we consider have a high organisational risk and potential significant impact.	

Introduction

This audit was agreed following a request from Corporate Governance Group and was initially intended to be an assurance piece of work. However, as the Publica transition has the potential for significant changes to the data protection provision and governance arrangements, it was agreed that an assurance report wouldn't be beneficial at this time. We have therefore prepared this advisory report with an overarching agreed action which incorporates all key findings and observations for the Council to consider. We will plan a follow-up audit in 2025/26.

WODC is classed as a 'Data Controller' under UK GDPR, and as such, they have greater responsibilities than 'Data Processors' (e.g. Publica). In addition to the suggestions which address the key findings of this report, we have suggested a brief process for WODC to enhance controls for their Data Controller obligations. Please see the Information Commissioners Office (ICO) website for more details and guidance.

1. Data Processing Impact Assessments (DPIAs) – Complete/review DPIAs for all services to establish and map why and how personal data is processed.
2. Governance arrangements – Establish the specific WODC Data Protection structure and reporting arrangements. The DPIAs should be used to support this.
3. Documentation – Review and update documentation to reflect specific WODC processes. Ensure consideration to shared roles and data sharing agreements, especially in relation to 3rd parties.

The Data Protection team (at the time of audit) was 2 part time employees who reported to the ICT Audit and Compliance Manager (designated Data Protection Officer (DPO) registered with the ICO for West Oxfordshire District Council, 2 partner Councils and Publica). It is recognised that a greater part of the Data Protection team's work was focussed on Subject Access Requests (SARs) and Freedom of Information (Fol) requests which made proactive work on the data breach process and business as usual challenging. Management wants to stress that there have been major improvements to the availability of Data Protection information (UK GDPR) and data breach policies etc. on the Council website.

We have subsequently been advised that Data Protection reporting mechanisms are in the process of being transferred to the Business Manager – Business Continuity, Governance and Risk.

Audit Scope

The audit included a review of:

- Policies and process for reporting/responding to a data breach
- Training provision for service areas
- The data breach register
- Data breach statistics
- Data breach communications

A data breach survey was issued to Assistant Directors, Business Managers and Heads of Service to provide additional insights.

Key Findings

Guidance for the Data Protection Team and Wider Organisation.

Whenever a data breach is reported, the Data Protection team must make assessments on risk, define remedial action and next steps. Decisions include:

- whether the breach should be reported to the ICO,
- which register the breach should be recorded on, and
- if they should be included in reporting statistics.

Our testing shows that there is an inconsistent process for dealing with reported breaches. For example, breaches on the register were not always supported with a completed form, risk assessments, and/or remedial actions noted. How breaches were communicated to stakeholders also varied. Data breach guidance is available to staff, but is in need of review and refresh, as errors and inconsistencies have been identified, these issues have been shared with the Data Protection Officer (DPO) and Chief Technology Officer (CTO).

Suggestion: Internal guidance/process notes detailing the steps to be taken when a data breach is reported should be developed for the Data Protection team. Developing this guidance will help to improve consistency and resilience and will support the development of any new team members.

A review and update of data breach guidance for the wider organisation should be undertaken to ensure the most up to date guidance is available to all staff.

Response: Data Protection will remain within Publica. An officer will be tasked with drafting guidelines and updating processes.

Data Breach Register

At the time of testing of the data breach register identified errors and inconsistencies. The register is compiled from data submitted on reporting forms but completed forms or further supporting information was not available for some of the test sample. Full details of the anomalies identified have been provided to the DPO and CTO.

Administration of the Data Breach Register has recently transferred to the BM – Business Continuity, Governance and Risk. Planned training (see section below), will help to ensure that all data breaches and near misses are reported through the correct process. IA can confirm that improvements have been made to the data reported in the data breach register.

Suggestion: The data breach reporting form and register should be reviewed and updated to ensure alignment with each other and with the Data Breach Policy. Updates to the form should ensure the parts to be completed by the reporter (e.g. description, date of the incident, etc) and the parts to be completed by the Data Protection team (e.g. unique reference, risk assessment, etc) are clearly marked.

Data Breach Registers are in need of review and refresh to ensure all data in respect of breaches, and near misses, are accurate and to allow for improved reporting arrangements.

Response: This will be included in the work being undertaken as above.

Data Breach Communication Arrangements

There is no formal arrangement in place for reporting data breaches to Publica and/or Council Officers. Corporate Governance Group (CGG) had raised concerns about the number of data breaches, quality and lack of associated information provided.

Suggestion: To ensure that expectations for reporting data breaches are clear for the Data Protection team and the organisations they serve, the BM – Business Continuity, Governance and Risk should agree data breach communication requirements with the Monitoring Officer and other key stakeholders (e.g. AD's, Business Managers/Heads of Service). Agreed data breach communication arrangements, should be reflected within relevant documentation. A review and approval process should be established for data breach communication agreements.

Response: This will be included in the work being undertaken as above. Furthermore, a written report will be created, and presented, at Corporate Governance Group.

Senior Information Risk Owner (SIRO)

The Data Breach Policy and related documentation references the SIRO and DPO as separate positions. But the DPO provided evidence to suggest that they currently have SIRO responsibilities, current ICO guidance suggests that these roles should be separate positions. With the transition of Publica services back into the Council, it may be appropriate to appoint a member of Senior Management to the SIRO role.

Response: The Administration of Data Protection has been transferred to the BM – Business Continuity and Risk. The WODC Director of Place is now the designated SIRO, all associated documentation and public facing information should be updated to reflect this change.

Data Breach Training

The Reporting of Personal Data Breaches Policy and Procedure states employees will be trained annually. Training is available on 2 separate platforms (Business Compliance Essentials and is included in some modules in Cyber Ninjas) and it is also included as part of induction training. But there is no requirement for annual completion for these courses. Survey results have highlighted that further data protection training would be beneficial. A respondent advised that when they feel it is a minor issue (for example when they need to redact a phone number or signature) they do not report it to the DPO. However, this approach breaches guidance that states a register of all breaches must be maintained. We have provided full details, to the DPO and CTO, of where improvements could be made to the Data Breach Training provision, to ensure a consistent approach/reporting is understood and followed by all. Cyber Ninjas refresher training has recently been rolled out to all staff for completion, elements of Data Protection are included in this training.

Suggestion: The Data Protection training provision should be reviewed and updated with consideration to the following:

1. Process for administering training.
2. Formal acknowledgement (e.g. electronic signature) of the Data Breach Policy.
3. Defining the action for follow-up of non-completion of training. The consequences for non-compliance should be clear.
4. Guidance for sharing information with 3rd parties including requirements for sharing with non-Publica/gov.uk email addresses.
5. Establishing a process for Identifying roles where additional data breach training is required.
6. Training provision communication process.
7. Any specific requirements for Councillors.
8. Alignment with relevant data protection policies.

Councillor's Training Completion

Councillors are Data Controllers and have specific data protection responsibilities. Failing to understand these responsibilities significantly increases the risk of data breaches.

Suggestion: Councillors should be contacted and reminded of their responsibilities as Data Controllers. The Local Government Association has created specific Data Protection guidance for Councillors which could be used to support explaining responsibilities.

Response: Councillors will be reminded of their responsibility through training and ICT information sessions.

Summary


Internal governance has not been sufficiently established for data breaches, therefore we have provided suggestions which, if implemented, will support the creation of a solid foundation of accessible and accurate information, processes and procedures. Furthermore, they will mitigate the risk of financial penalties and reputational damage to the Council/Publica from non-compliance with ICO reporting requirements.

Human Resources – Final Report – December 2024

Audit Objective

To provide assurance that staff absence management is operated in accordance with agreed policy/procedure and statutory regulations.


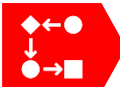


Executive Summary

	Assurance Opinion	Management Actions		Organisational Risk Assessment	Medium
	The advice provided in this report encompasses risk analysis and evaluation based on current activity/operations. Please see the conclusions box for details of why an advisory report has been used.	Priority 1	2	Our audit work includes areas that we consider have a medium organisational risk and potential impact.	
		Priority 2	1		
		Priority 3	1		
		Total	4		

NB: The Key Conclusions below are a reflection of the audit at the time of fieldwork: April-June 2024.

Since the audit, we have been advised that work has been undertaken to mitigate against the risks identified below. These areas have been addressed since the draft report was issued, and therefore have not been tested, but will be followed up as part of our standard follow up process.

Key Conclusions

	There was no clear corporate monitoring of sickness absence reporting undertaken by HR at the time of the audit. Reliance was placed on managers recording absence data in the BW system correctly. As an HR system BW is limited, and there are a number of workarounds required to make it work as needed. Internal reporting may be based on unreliable data and could lead to flawed decision making.
	There are different approaches across Publica for the management and reporting of sickness absence. We have made some suggestions / observations which the Council could adopt for their management of sickness reporting. As well as risking reporting unreliable data, there is a risk of inaccurate sick pay, employees being treated unfairly, and reputational damage. Also, managers risk failing in their duty of care towards their team members.
	The Sickness Absence Policy and Procedure (2023) states that a self-certification form should be completed for sickness of seven calendar days or less. At the time of the audit this form had not been created, but it has since been finalised and introduced. Also, the form could be used as a basis for the return to work meeting allowing opportunity to discuss wellbeing and any concerns which may arise. And if there is challenge by an employee for example, reasons for/length of absences, etc, the form could be used as evidence.
	The guidance on the 'Managers Support' webpage of the Publica Portal requires updating. This risks managers following out of date guidance which may / may not agree with the 2023 approved policies and procedures.

Audit Scope

The audit included a review of:

- Absence Management Roles and Responsibilities
- Absence Monitoring and Reporting
- Data Analytics to identify anomalies and/or confirm reporting is based on sound data.
- Sickness absence between September 2022 – February 2024 was analysed/tested.

A survey was issued to a sample of Assistant Directors, Business Managers and Heads of Service to provide additional insights on management, recording and monitoring of absences.



Training on administering both Sickness Absence policies was delivered to Managers in December 2023 following the wider review of all HR policies. All new managers will receive training on these policies and how to record absence in BW as part of their induction. All Managers we spoke to knew where to find relevant policies. Since the audit, a reminder has been issued to managers on the current process of sickness reporting.

Summary

This audit was requested by the HR Manager and was initially undertaken as an assurance piece of work. However, as the Publica transition has the potential for significant changes to HR arrangements, it was agreed that an assurance report would not add value at this time.

Instead, we have prepared this advisory report and have agreed actions with the HR Manager for employees remaining in Publica.

Going forward each Council will need to consider arrangements for their own staff and so the findings from this review should help inform future arrangements for each of the Council's staff.

We suggest that the following observations are explored with a view to making the absence reporting and monitoring process more effective:

- Consideration could be given to amalgamating the Publica Sickness Absence Policy and Procedure (2023) with the Publica Long Term Sickness Absence Policy and Procedure (2023), so all sickness absence guidance is contained in one place and limits unnecessary duplication. This will help to ensure that there is no confusion over how sickness absence is managed. We have been advised that this is in progress, and a new (combined) policy will be available shortly to Publica and Council Officers.
- We accept that the BW system is not an intuitive HR system and that work arounds have had to be introduced, but if managers were given additional training and HR support to ensure everyone operates a consistent process, then perhaps an alternative system (Resident Services absence line) may not be required.
- But, if, in the future, a new management system is implemented, then it is essential that BW data is robust so as not to transfer inaccurate data into a new system.

Additional observations regarding employee welfare were identified as follows:

- There is no guidance available on the expectations surrounding how Managers should keep track of their team's whereabouts whilst hybrid working (working from home). Not knowing their whereabouts could have a detrimental impact on more than just the accuracy of sickness reporting.
- There is no standard way of ensuring that the whereabouts of Officers out in the field is accounted for, e.g., clocking in and out and using a check in/check out system between site visits. There is a risk that lone workers could be in danger during work time, and Publica would not know or be able to help. We have made the H&S Business Partner aware of this.

If the actions to address the key findings above are implemented, then this will help introduce a stronger control environment and improve the accuracy of data being reported. We will revisit this area to undertake a follow up review in due course.

Revenues and Benefits (Ctax and NNDR) – Final Report – January 2025

Audit Objective

To ensure key financial system controls are operating effectively for Council Tax and Business Rates and that opportunities for error, fraud or corruption are minimised.

Executive Summary



Assurance Opinion

The review highlighted a generally sound system of governance, risk management and control in place. We identified some issues, non-compliance or scope for improvement which may put at risk the achievement of objectives.

Management Actions

Priority 1	0
Priority 2	1
Priority 3	1
Total	2

Organisational Risk Assessment

Low

Our audit work includes areas that we consider have a low organisational risk and potential impact. We believe the key audit conclusions and any resulting outcomes still merit attention but could be addressed by service management in their area of responsibility.

Key Conclusions



There are values in the Suspense Account dating back to 2020. Revenues and Benefits Officers will liaise with the S151 Officer to decide what action should be taken with historical suspense account entries.



Review of the 2024 Suspense Account found 2 negative values where corresponding positive values could not be identified. The Assurance Manager will liaise with colleagues in Finance to ensure all suspense account entries have an audit trail to support they have been transferred to the correct account.



1 agreed action from last year's audit is still outstanding. The Revenues Manager advised basic procedure guidance is being drafted and officer training will be completed by the end of 2024.



- There is no separation of duties when adding or removing a property in Civica, but evidence was supplied to support Revenues Officers reconcile properties in Civica to Valuation Office Agency (VOA) records.
- We received satisfactory responses to our testing queries.
- Evidence was supplied to support CTax discounts and exemptions are reviewed.
- Regular cash reconciliations are undertaken.

Audit Scope

Discussions were held with Publica Revenues and Benefits Officers and evidence sought to support statements made. We reviewed the following.

- CTax/NNDR – Valuation process, and discounts and exemptions.
- Key control testing – financial reconciliations and variance reporting.
- Follow up of previously agreed actions.

Sample testing was undertaken on a random sample of CTax and NNDR accounts to ensure they had been applied in accordance with procedure.

Other Relevant Information

The assurance we have given is specific to the areas we have reviewed this year.

There are a large number of closed accounts in credit at the Council, but evidence has been supplied to support work is being done to trace account holders and refund them. Analysis of closed Council Tax accounts in credit was undertaken in November 2022, and comparing this to the data provided for our 2024 audit we can report a 40% reduction of the number of closed accounts in credit. Consideration should be given to how long these credits remain on the system and how long officers spend trying to trace account holders before credits are written on, to ensure the benefits outweigh costs to the service area.


The Assurance Manager advised there are currently no quality assurance checks undertaken on valuations or discounts and exemptions due to how Civica is configured, but they plan to introduce these soon.


All NNDR discounts and exemptions are not reviewed at the Council; the Revenues Manager advised this is because they felt very few of them would change. Evidence was supplied to support Discretionary Rate Relief is approved by Members. And the Retail, Hospitality and Leisure Relief Scheme and Small Business Rate Relief are managed using Civica system parameters.

Sample testing found VOA wait times are impacting the time it takes for valuations to be confirmed in the Council systems.

Revenues and Benefits (Housing Benefit and Council Tax Support) – Final Report – January 2025

Audit Objective To ensure key financial system controls are operating effectively for Housing Benefits and Council Tax Support and that opportunities for error, fraud or corruption are minimised.

Executive Summary											
	Assurance Opinion The review confirmed a sound system of governance, risk management and control, with internal controls operating effectively and being consistently applied to support the achievement of objectives.	Management Actions	Organisational Risk Assessment								
		<table border="1"> <tr> <td style="background-color: red; color: white;">Priority 1</td> <td style="text-align: center;">0</td> </tr> <tr> <td style="background-color: yellow;">Priority 2</td> <td style="text-align: center;">0</td> </tr> <tr> <td style="background-color: blue;">Priority 3</td> <td style="text-align: center;">0</td> </tr> <tr> <td style="background-color: #000080; color: white;">Total</td> <td style="text-align: center;">0</td> </tr> </table>	Priority 1	0	Priority 2	0	Priority 3	0	Total	0	Low A sound system of governance, risk management and control exist, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
	Priority 1	0									
	Priority 2	0									
Priority 3	0										
Total	0										

Key Conclusions		Audit Scope
 <ul style="list-style-type: none"> Members have approved the 2024/25 CTS scheme. Quality Assurance checks are undertaken on HB and CTS claims. We received satisfactory responses to our testing queries. Evidence has been supplied to support reconciliations are undertaken. Evidence has been supplied to support HB overpayments are monitored. 		Discussions were held with Publica Revenues and Benefits Officers and evidence sought to support statements made. We reviewed the following. <ul style="list-style-type: none"> HB & CTS – Application process, passported claims and evidence verification. Key control testing – financial reconciliations and variance reporting. Follow up of previously agreed actions. Sample testing was undertaken on a random sample of HB and CTS claims to ensure they had been applied in accordance with procedure.

Other Relevant Information

The assurance we have given is specific to the areas we have reviewed this year.

At the time of audit work (October 2024) there was an unexplained difference of £308.81 on the CTS reconciliation, and the Assurance Manager confirmed this would be discussed with the Publica Business Partner Accountant to identify and explain the discrepancy. At the time of report writing (December 2024) the Assurance Manager advised the account has been identified and a call has been raised with OpenRevenues.

During testing of housing benefit overpayments, we identified a few small values which had not been written off as expected. We were advised by the Benefits Team Leader these had been included in the next write offs to go to the S151 officer for approval.

