Joint Audit and Governance Committee

Report of Interim Internal Audit Manager

Author: Richard Green

Telephone: 01235 422430

Textphone: 18001 01235 422430

E-mail: Richard.green@southandvale.gov.uk

SODC cabinet member responsible: Councillor Leigh Rawlins

Tel: 01189 722565

E-mail: leigh.rawlins@southoxon.gov.uk

VWHDC cabinet member responsible: Councillor Andy Crawford

Telephone: 01235 772134

E-mail: andy.crawford@whitehorsedc.gov.uk

To: Joint Audit and Governance Committee

DATE: 26 January 2021

Internal audit activity report quarter three 2020/21

Recommendation

That members note the content of the report

Purpose of report

1. The purpose of this report is to summarise the outcomes of recent internal audit activity at both councils for the committee to consider. The committee is asked to review the report and the main issues arising and seek assurance that action will be/has been taken where necessary.

2. The contact officer for this report is Richard Green Interim Internal Audit Manager for South Oxfordshire District Council (SODC) and Vale of White Horse District Council (VWHDC), telephone 07849 574860.

Strategic objectives

3. Delivery of an effective internal audit function will support the councils in meeting their strategic objectives.

Background

4. Internal audit is an independent assurance function that primarily provides an objective opinion on the degree to which the internal control environment supports and promotes the achievements of the council's objectives. It assists the councils by evaluating the adequacy of governance, risk management, controls and use of resources through its planned audit work and recommending improvements where necessary. After each audit assignment, internal audit has a duty to report to management its findings on the control environment and risk exposure and recommend changes for improvements where applicable. Managers are responsible for considering audit reports and taking the appropriate action to address control weaknesses.

5. Assurance ratings given by internal audit indicate the following:

   Full assurance: There is a good system of internal control designed to meet the system objectives and the controls are being consistently applied.

   Substantial assurance: There is a sound system of internal control designed to meet the system objectives and the controls are being applied.

   Satisfactory assurance: There is basically a sound system of internal control although there are some minor weaknesses and/or there is evidence that the level of non-compliance may put some minor system objectives at risk.

   Limited assurance: There are some weaknesses in the adequacy of the internal control system which put the system objectives at risk and/or the level of non-compliance puts some of the system objectives at risk.

   Nil assurance: Control is weak leaving the system open to significant error or abuse and/or there is significant non-compliance with basic controls.

6. Each recommendation is given one of the following risk ratings:

   High Risk: Fundamental control weakness for senior management action

   Medium Risk: Other control weakness for local management action

   Low Risk: Recommended best practice to improve overall control

Completed audit reports

7. As at 07 January 2021, since the last joint audit and governance committee meeting the following audits and follow up reviews have been completed:

   Completed Audits: 7
   Full Assurance: 0
   Substantial Assurance: 0

Satisfactory Assurance: 5
Limited Assurance: 2
Nil Assurance: 0

Audit Area	Assurance Rating	Total Recs	High Risk	No. Agreed	Medium Risk	No. Agreed	Low Risk	No. Agreed
Joint								
1. Information Security 19/20 (**appendix 1**)	Limited*	**7**	5	5	2	2	0	0
2. Housing Benefits & CTRS 19/20 – updated** (**appendix 1**)	Limited	**3**	1	1	0	0	2	2
3. Data Protection / GDPR 19/20	Satisfactory	**8**	0	0	3	3	5	5
4. Procurement 19/20	Satisfactory	**4**	0	0	2	2	2	2
5. Lone Working & Officer Security 19/20	Satisfactory	**12**	0	0	4	4	8	8
6. General Ledger 19/20	Satisfactory	**10**	0	0	4	4	6	6
7. HR Management & Reporting 20/21	Satisfactory	**12**			8	8	4	4
SODC								
None								
VWHDC								
None								

* *Under normal circumstances, Capita would be invited to the JAGC to discuss any limited assurance audit reports for Capita service offerings. However, Capita are not in attendance at this virtual meeting. The interim internal audit manager will take away any questions the committee may have for Capita and will obtain responses in due course.*

*** At the 22 September 2020 JAGC meeting, members raised several questions in relation to recommendation 3, review of overpayments. The recommendation wording has been updated in response to these questions and is presented at this committee meeting for information purposes only.*

8. The work on the Covid 19 Response Governance Review was started at the end of November and the Terms of Reference and Objectives have been agreed. The work has commenced but is still at an early stage and there are no significant findings to report at this time.

Follow Up Reviews

Audit Area	Initial Assurance Given	No. of Recs	Implemented	Partly Implemented	Not Implemented	Ongoing	No longer applicable
Joint							
Development Management 19/20	Satisfactory	8	4	3	1	0	0
Elections & Election Payments 19/20	Limited	5	5	0	0	0	0
SODC							
None							
VWHDC							
None							

9. **Appendix 1** of this report sets out the key points and findings relating to the completed audits which have received limited or nil assurance, and satisfactory or full assurance reports which members have asked to be presented to committee.

10. Members of the committee are asked to seek assurance from the internal audit reports and/or respective managers that the agreed actions have been or will be undertaken where necessary.

11. A copy of each report has been sent to the appropriate service manager, the section 151 officer and the relevant member portfolio holder. In addition, reports are now published on the councils' intranet and limited assurance reports are reviewed by the strategic management team.

12. Internal audit continues to carry out a six month follow up on all non-key financial audits to establish the implementation status of agreed recommendations. All key financial system recommendations are followed up as part of the annual assurance cycle.

Financial implications

13. There are no financial implications attached to this report.

Legal implications

14. None.

Risks

15. Identification of risk is an integral part of all audits.

Richard Green
INTERIM INTERNAL AUDIT MANAGER

APPENDIX 1

1. Information Security 2019/20

MANAGEMENT SUMMARY

1. INTRODUCTION

1.1 This report details the internal audit review of procedures, controls and the management of risk in relation to information security. The audit has been undertaken in accordance with the 2019/2020 audit plan agreed with the joint audit and governance committee of South Oxfordshire District Council (SODC) and Vale of White Horse District Council (VWHDC). The audit has a priority score of 21. The audit approach is provided in the audit framework in Appendix 1.

1.2 The following areas have been covered during the course of this review to provide assurance that:

- the councils have an adequate information/cyber security framework, policies, procedures and guidance in place;
- there are adequate controls in place for accessing and sharing information with other service areas, contractors and partners;
- council officers and members are aware of cyber and information security principles and policies;
- appropriate controls to prevent data loss and unauthorised access are in place;
- robust procedures are in place in the event of a cyber/information security incident and are regularly tested;
- key learning points and recommended actions from the recent corporate fraud and cyber security risk assessment have been addressed.

2. BACKGROUND

2.1 Information security refers to the processes and methodologies which are designed and implemented to protect print, electronic, or any other form of confidential, private and sensitive information or data from unauthorised access, use, misuse, disclosure, destruction, modification, or disruption.

2.2 Cyber security is the practice of defending computers, servers, mobile devices, electronic systems, networks and data from malicious attacks.

2.3 The councils have a statutory duty under the following legislations and associated regulations in relation to the use, storing and handling of information:

- GDPR 2018;
- Data Protection Act 1998;
- Freedom of Information Act 2000;
- ENISA (the European Union Agency for Cybersecurity) and information and communications technology cybersecurity certification and repealing Regulations 2019;

- Privacy and Electronic Communications Regulations 2003;
- Regularly of Investigatory Powers Act 2000;
- Copyright, Designs and Patents Act 1988;
- Computer Misuse Act 1990;
- Human Rights Act 1998;
- Counter-Terrorism and Security Act 2015;
- Protection of Children Act 1978;
- Criminal Justice and Immigration Act 2008;
- Defamation Act 2013;
- Equality Act 2010.
- Terrorism Act 2006;
- Limitation Act 1980;
- Official Secrets Act 1989;
- Malicious Communications Act 1988;
- Digital Economy Act 2010;
- Privacy and Electronic Communications Regulations 2011;
- Police and Justice Act 2006;
- Obscene Publication Act 1964;
- Police and Criminal Evidence Act 1984;
- Prevention of Terrorism Act 2005.

3. PREVIOUS AUDIT REPORTS

3.1 Information security has not previously been subject to an internal audit review. However, a corporate fraud and cyber security risk assessment was undertaken in March 2019 and reported to the Joint Audit and Governance Committee in October 2019. 19 recommendations were made, of which nine recommendations related to cyber security. Of the nine recommendations, four were high risk, two medium risk, one low risk and two very low risk recommendations.

3.2 Of the nine recommendations, five have not been implemented and five recommendations are no longer applicable. Of the four recommendations, three have been superseded by recommendations raised in this audit and one recommendation has been restated as a result of our work in this area (Rec 5).

4. 2019/2020 AUDIT ASSURANCE

4.1 **Limited assurance:** There are some weaknesses in the adequacy of the internal control system which put the system objectives at risk and/or the level of non-compliance puts some of the system objectives at risk.

4.2 Seven recommendations have been raised in this review. Four high risk, one medium risk and two low risk.

5. MAIN FINDINGS

5.1 Framework, policies and procedures

5.1.1 As part of the five councils' partnership (5CP), cyber security is managed by Capita and a service delivery plan (SDP) is in place outlining the service that will be provided. A 5CP client relationship team is in place to ensure that an acceptable level of service is provided by Capita to the councils. A security working group is in place, which meet on a monthly basis. The group consists of Capita IT and representatives from each of the five councils and any IT security breaches are discussed.

5.1.2 The councils' do not have in place an information/cyber security strategy. Capita IT have in place cyber security policies and procedures, covering a range of topics; however, these are only available to Capita IT and not council staff. The councils' intranet (Jarvis) publishes limited cyber security information for officers, including how officers can remain vigilant to cyber security risks.

5.1.4 Area assurance: Limited
Two recommendations have been made as a result of our work in this area (Recs 1 and 2).

5.2 Accessing and sharing information

5.2.1 Access to the councils' network is restricted to council staff, fixed term contract (FTC) staff and relevant Capita staff. Staff have access to network drives specific to their service area. If access is required for another service area's network drive, approval is required from the officer's service manager prior to authorisation by Capita IT.

5.2.2 Section IT406 of the Capita' SDP states that Capita shall establish and enforce good practice to protect personal data from being sent insecurely and incorrectly. Sensitive/confidential information is commonly transferred between service areas via email. Prior to payroll and HR coming back in-house (effective 1 April 2020), Capita previously sent payroll reports to the councils via secure email, which required a password. Currently, it was confirmed that the payroll files are emailed internally without encryption. Testing also found that sensitive/confidential information from a council email account to a personal email account could be sent. In addition, we were successful in uploading this information directly to a personal email account whilst on the councils' network.

5.2.4 Area assurance: Limited
One recommendation has been made as a result of our work in this area (Rec 3).

5.3 Cyber and information security awareness

5.3.1 Cyber security awareness guidance is available to both officers and councillors via the councils' intranet (Jarvis). Guidance includes, password management, using of public WIFI, and awareness scamming and ransoms. Councillors, as part of their induction, following the local elections in May 2019, were also provided with an IT guide. From review the IT guide, internal audit was satisfied that sufficient guidance is available to councillors.

5.3.2 The councils, however, have not provided officers with information/cyber security awareness sessions/ training. As part of induction, councillors are provided IT training; however, review of the training presentation found that the presentation did not include any information on cyber security awareness.

5.3.4 Area assurance: Substantial

One recommendation has been made as a result of our work in this area (Rec 4).

5.4 **Data loss and unauthorised access**

5.4.1 Access to the councils' network is restricted to council employees and contractors. For new employees, leavers and contractors, a request form must be completed and submitted to Capita helpdesk to either obtain or revoke network access. Capita has in place a joiners, movers and leavers IT process reference guide, which sufficiently details the process to be undertaken to ensure that only authorised personnel obtain access to network and to certain drives. It is noted that access control to systems that hold sensitive information, i.e. ResourceLink, Agresso, etc. is not reviewed as part of this audit as they are reviewed as part of the payroll, general ledgers and pro-active anti-fraud audit reviews. No issues were raised during both the payroll and general ledger audits, however during the pro-active anti-fraud review issues were raised in relation to user access.

5.4.2 As mentioned in objective three, limited cyber security guidance is available on Jarvis. One area of guidance relates to workstations and passwords, which states to lock the workstation every time left unattended. For three days, over a two-week period, internal audit and the assurance team leader undertook a walk around the Milton Park office and found that 39 (13 per day) workstations were unlocked when unattended, increasing the risk of unauthorised personnel viewing sensitive information.

5.4.3 Area assurance: Satisfactory
Two recommendations have been made as a result of our work in this area (Recs 5 and 6).

5.5 **Cyber and information security incidents**

5.5.1 Cyber security incident is a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted access to a system or systems. Capita IT has in place procedures detailing the process for reporting cyber/information security incidents, which has been agreed by the five councils. However, the procedures have not been made available to council officers. Cyber security incidents are recorded and discussed during the security working group, between Capita IT and representatives from the councils.

5.5.2 The councils currently do not have a disaster recovery plan in place in the event of a cyber/ information security incident. It is noted that Capita IT have a generic plan, which was rejected by the councils as it did not fulfil the councils' requirements. The Local Government Association (LGA) require local government to have an in-house cyber security expert, and in February 2020, offered both SODC and VWHDC funding to train a member of staff.

5.5.3 Area assurance: Limited
One recommendation has been made as a result of our work in this area (Rec 7).

6. ACKNOWLEDGEMENTS

6.1 Internal audit would like to take this opportunity to thank all staff involved for their assistance with the audit.

7. CATEGORISATION OF RECOMMENDATIONS

7.1 To assist management in using our reports, we have categorised our recommendations according to their level of priority as follows:

High risk	Fundamental control weakness for senior management action	**Recs 1, 3, 4, 6 and 7**
Medium risk	Other control weakness for local management action	**Recs 2 and 5**
Low risk	Recommended best practice to improve overall control	

OBSERVATIONS AND RECOMMENDATIONS

FRAMEWORK, POLICIES AND PROCEDURES

1. Cyber security strategy **(High Risk)**

Rationale	Recommendation	Responsibility
Best Practice A cyber security strategy in place, which documents a plan of actions designed to improve the councils' approach and resilience to infrastructure and services and establishes a range of objectives and priorities that should be achieved in a specific timeframe. Findings The councils do not have a cyber security strategy in place. The strategy is a plan of actions designed to improve the security and resilience of the councils' infrastructures and services. It is a high-level top-down approach to cyber security that establishes a range of objectives and priorities that should be achieved in a specific timeframe. Risk If a cyber security strategy is not in place, there is a risk of security not being managed appropriately	a) Develop a cyber security strategy and obtain approval in line with the councils' Constitution. b) Communicate the approved cyber security strategy to council officers and Capita IT.	Interim IT Programmes Manager

resulting in possible breaches to the councils' network.		
Management Response		**Implementation Due Date**
Recommendation is **Agreed in Principle** There is a dependency on aligning with the Capita 5CP cyber security strategy which will impact the councils' ability to devise their own strategy. Management response: Interim IT Programmes Manager		31 July 2021

2. Jarvis information (Medium Risk)

Rationale	Recommendation	Responsibility
<u>Best Practice</u> The cyber security page, on the intranet (Jarvis), provides the relevant details required to ensure officers are cyber aware. Jarvis also has attached cyber security policies and procedures. <u>Findings</u> Capita IT has cyber security policies and procedures in place; however, from review of Jarvis, internal audit found that the policies and procedures are not available to council officers. Internal audit reviewed the 'Be Cyber Secure' page on Jarvis and found that information in relation to the requirement to not send council information to personal emails was not included. <u>Risk</u> If cyber security policies and procedures are not widely available, officers may lack awareness of their individual responsibilities and requirements to stay cyber safe, which may increase the risk of a network breach.	a) Obtain copies of the Capita cyber security policies and procedures and communicate to council staff via the councils' intranet (Jarvis). b) Review and update information published on the councils' intranet (Jarvis) to document the risks of sending council information to personal emails/devices.	Interim IT Programmes Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed** Ensure regular review of all policies via Capita data security team and upload on to Jarvis. Re-establish cyber awareness campaign. Additional modules for LEAH are being added to provide cyber-security training for staff. Management response: Interim IT Programmes Manager		31 March 2021

ACCESSING AND SHARING INFORMATION

3. Network firewall (High Risk)

Rationale	Recommendation	Responsibility
Best Practice The network firewall is secure, so that sensitive/confidential information cannot be uploaded onto or sent to personal email accounts. Findings IT security service specification (IT406) states to protect personal data from being sent insecurely or incorrectly. Internal audit, along with the IT infrastructure lead, developed a dummy payroll file and: 1. uploaded it to a personal email address; 2. emailed the file to a personal email address. Review found that payroll file can be uploaded and emailed to personal email addresses. It is noted the internal audit also managed to open payroll file using a personal device. Risk If the network firewall is not secure and data files can be uploaded to personal email addresses, there is a risk of data loss, unauthorised usage, or for sale to third parties.	Review controls within the councils' network firewall to prevent sensitive/confidential information being uploaded or sent to personal email accounts.	Interim IT Programmes Manager

Management Response	Implementation Due Date
Recommendation is **Agreed in Principle** Blocking of personal data from being emailed out to a personal account as opposed to sending personal information to a legitimate recipient, for example housing association, needs to have rules set, these need to be agreed with Capita. Management response: Interim IT Programmes Manager	31 March 2021

CYBER SECURITY AWARENESS

4. Cyber security awareness (High Risk)

Rationale	Recommendation	Responsibility
Best Practice All officers and councillors have been provided with cyber security awareness sessions.	Establish regular cyber security awareness sessions, which are mandatory for officers and councillors.	Interim IT Programmes Manager/ Emergency Planning Officer

Findings Cyber security awareness sessions have not been set up or provided to officers or councillors. Through discussion, it was noted that the assurance team have looked into the possibility of provided these training sessions; however, COVID-19 and lockdown has prevented this. Risk If councils' do not provide cyber security awareness sessions, there is a risk that officers and councillors are not aware of what is required to stay cyber safe, increasing the potential for a cyber security incident/breach.		
Management Response		**Implementation Due Date**
Recommendation is **Agreed** Ensure regular review of all policies via Capita data security team and upload on to Jarvis. Re-establish cyber awareness campaign. New staff awareness and training material is being added to LEAH which will form part of the staff induction process. Management response: Interim IT Programmes Manager		31 March 2021

DATA LOSS AND UNAUTHORISED ACCESS

5. Active directory management (Medium Risk)

Rationale	Recommendation	Responsibility
Best Practice Procedures for management of the active directory are in place. Findings Whilst a joiner, mover and leavers (JML) process is in place to remove users from the active directory, there are many locally administered systems in use across the councils that are not linked to the JML process, hence there is an increased risk that the users of these systems are not reviewed and reconciled to the current employee list. Risk If the active directory is not kept updated and linked to the JML process in order to ensure users are removed or access rights are configured correctly, there is a risk that systems can be accessed by	Develop clearly defined procedures for management of the active directory and communication to officers.	IT Development Manager/ HR Manager

unauthorised individuals outside their allocated permissions.		
Management Response		**Implementation Due Date**
Recommendation is **Agreed in Principle** Spot-check AD is being updated as part of JML, but accuracy is dependent upon HR submitting the form correctly. Management response: IT Development Manager/ HR Manager		31 March 2021

6. Laptop/desktop security (High Risk)

Rationale	Recommendation	Responsibility
Best Practice Council officers and contractors lock their workstation each time they are left unattended. Findings During a two-week period in September 2019, internal audit performed three office walkarounds on three different days to establish whether any laptops/desktops were left unlocked and unattended. Internal audit found that on 39 occasions, laptops/desktops were left unlocked when unattended (13 workstations per walkaround). Risk If laptops/desktops are left unlocked when unattended, there is a risk of officers viewing confidential/sensitive documents to which they are authorised to do so.	Issue regular reminders to officers and contractors of the requirement to lock their laptop/ desktop when left unattended.	Interim IT Programmes Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed** Ensure regular review of all policies via Capita data security team and upload on to Jarvis. Re-establish cyber awareness campaign. Staff communications to remind people to lock laptops when unattended - especially with remote and offsite working now a normal practice. Management response: Interim IT Programmes Manager		31 March 2021

CYBER/INFORMATION SECURITY INCIDENT

7. Disaster recovery plan (High Risk)

Rationale	Recommendation	Responsibility
Best Practice A disaster recovery plan is in place, which is regularly tested.	a) Develop a disaster recovery plan to prepare for a cyber/ information security incident.	IT Programme Manager/ Emergency Planning Officer

Findings Internal audit established, from conversations with both the assurance team leader and the IT infrastructure lead, that there is currently no disaster recovery plan in place to assist in the event of a cyber/ information security incident. Risk If a disaster recovery plan is not in place, there is a risk that the councils fail to respond appropriately and in a timely manner to recover councils' services, following an incident/ disaster.	b) Once a disaster recovery plan is in place, undertake regular testing to ensure that the plan is fit for purpose.	
Management Response		**Implementation Due Date**
Recommendation is **Agreed in Principal** There is a dependency on aligning with the Capita 5CP cyber incident plan and the wider 5CPs IT infrastructure which will impact the councils' ability to devise their own plan. Management response: Customer Assurance Manager/ Interim IT Programmes Manager		31 March 2021

2. Housing Benefits & CTRS 2019/20 – updated

The initial report for this review was presented to JAGC in September 2020 but there was concerns regarding the values of the errors identified and the sampling methods applied.
To address these concerns further tests were undertaken using a statistical random sample of overpayments. No further issues were identified and this report is updated to reflect this additional testing.
As requested, the methodology used to select samples has been reviewed and a separate paper is included setting out the revised approach.

MANAGEMENT SUMMARY

1 INTRODUCTION

1.1 This report details the internal audit review of procedures, controls and the management of risk in relation to housing benefits (HB) and council tax reduction scheme (CTRS). The audit has been undertaken in accordance with the 2019/2020 audit plan agreed with the audit and governance committee of South Oxfordshire District Council (SODC) and Vale of White Horse District Council (VWHDC). The audit has a priority score of 21. The audit approach is provided in the audit framework in Appendix 1.

1.2 The following areas have been covered during the course of this review to provide assurance that:

- the administration of benefits is up to date, including guidance, procedures and training for officers carrying out assessments, so the process runs smoothly;
- benefits assessments are correctly calculated, promptly undertaken and adequate quality checks take place;
- payments of housing benefits and CTRS are managed appropriately with suitable supporting documentation;
- there is a suitable mechanism to identify and recover benefit overpayments;
- there is an adequate audit trail to substantiate the figures on the housing benefits subsidy claim, the claim is properly completed, and the figures included are accurate;
- processes are in place to prevent and detect fraud and for fraud referrals to the Department of Work and Pensions (DWP); and
- performance is appropriately recorded, monitored and reported.

2. BACKGROUND

2.1 Housing benefits and CTRS are means tested schemes to help those on low income pay their rent and/or council tax. The DWP set the rules for the housing benefits calculations which is dependent upon income and prescribed needs allowances. CTRS is the councils' own scheme that utilises the same rules as for housing benefits. The DWP has been introducing Universal

Credit to replace housing benefits and other state benefits with a single payment, at SODC and VWHDC since 2015.

2.2 Capita continues to provide the HB and CTRS service for the councils and, since 1 August 2016 this is delivered within the 5 Councils Partnership (5CP). A client team was in place providing HB and CTRS oversight for all of the 5CP councils at the outset of the 5CP contract. During November 2018, this was scaled down and resources returned to the council to retain oversight and perform functions that cannot be outsourced, such as 10% checks on assessments. The councils' now have an in-house revenues and benefits team and, as far as the 5CP contract overall, there is still oversight managed through the Client Relationship Director. The councils' representative for issues affecting all councils in the contract is the Head of Partnerships and Insight.

2.3 Housing benefits and CTRS is managed through the Advantage system. As at January 2020 the case reported caseload was:

	SODC	VWHDC
Housing benefits	5,214	5,246
CTRS	5,375	5,214
Net (some claims are for both housing benefits and CTS)	6,181	6,104

3. PREVIOUS AUDIT REPORTS

3.1 Housing benefits and CTRS was last subject to an internal audit review in March 2019 and seven recommendations were raised. All seven recommendations were agreed. A substantial assurance opinion was issued.

3.2 Of the seven recommendations, five have been implemented and two have not been implemented and are restated as part of this review (Recs 1 and 2).

4. 2019/2020 AUDIT ASSURANCE

4.1 **Limited assurance:** There are some weaknesses in the adequacy of the internal control system which put the system objectives at risk and/or the level of non-compliance puts some of the system objectives at risk.

4.2 One recommendation has been raised and two previous recommendations have been restated in this review. One high risk and two low risk.

5. MAIN FINDINGS

5.1 Procedures

5.1.1 Capita maintain a comprehensive set of 32 training manuals, which also act as procedures. The training manuals describe how to use the Advantage system to process housing benefits and CTRS claims. Capita has a training programme ranging from full new starter training to ongoing

refresher training. There have been no new starters since the previous audit review. The five Councils Partnership (5CP) contract specification sets out service delivery requirements including performance indicators.

5.1.2 The councils' revenues and benefits team maintain oversight of housing benefits and CTS service delivery, perform statutory checks and manage discretionary housing payments (DHP). It is noted that the DHP is an award to people in receipt of HB or the housing element of Universal Credit to help with housing costs where extra financial assistance is needed. The government allocates an annual allocation and sets a maximum that can be spent.

5.1.3 An online housing benefits and CTRS application form is made available through each council's website in addition to a PDF version of the application form. Claimants can apply for HB through DWP but that will not be a claim for CTRS. Therefore, claimants are asked to sign a single page stating their intention to claim CTRS as well as HB. It was noted that there is no reference to privacy notices or other data protection information on either the housing benefits/CTRS or DHP application or the councils' webpages.

5.1.4 Applicants are encouraged to personally bring sensitive documents supporting their claim to the council offices rather than send them via post. Should items be received through the post at either the council offices or at Capita's Erith offices they are returned by recorded delivery.

5.1.5 Area assurance: Substantial
One previous recommendation has been restated as a result of our work (Rec 1).

5.2 **Benefit assessments**

5.2.1 All housing benefits and/or CTRS applicants are required to complete an application form and provide supporting evidence attached to help prove identity and financial status (see 5.1.3). This information is assessed and input onto the Advantage system by Capita's benefits assessors' teams. Once the required financial information is entered onto Advantage, it automatically calculates the housing and CTRS for approved claimants. The calculation of benefits depends upon specific values (benefits parameters) which are saved within the benefits system and are used in benefit calculations, e.g. personal allowances for those aged 18-25. Internal audit selected a sample of 20 housing benefits uprating's, from DWP circular A8/2018, against housing benefits annual billing parameters and review confirmed that the housing benefits parameters were appropriately uploaded onto Advantage for both SODC and VWHDC.

5.2.2 In 2019/2020 to date (February 2020), there were 914 (455 SODC and 459 VWHDC) new housing benefits and/or council tax reduction scheme (CTRS) claims. A random sample of 40 (20 SODC and 20 VWHDC) new housing benefit claims and CTRS claims were to ensure that the assessments were undertaken in line with the relevant guidelines. Review confirmed that all claim forms were signed accordingly by the claimant, adequate supporting documentation was submitted to support the claim,

and, Capita assessed and responded to all claimants within 14 days of receiving all supporting documentation.

5.2.3 Capita provide the councils' revenues and benefits team with a daily report of the claims that have been assessed and a random 10 per cent sample is selected to quality check. Review of quality checks for one week (January 2020) confirmed that 10% are undertaken by the councils' revenues and benefits team, in line with The Contracting Out Order 2002.

5.2.4 Area assurance: Full
No recommendations have been made as a result of our work in this area.

5.3 **Housing benefits and CTRS payments**

5.3.1 Payments of HB and CTRS are made via BACS or cheque at varying frequencies (e.g. fortnightly, four weekly or monthly) depending on the claimant. Payment runs are undertaken on a weekly basis and review of two (one SODC and one VWHDC) payment runs confirmed that there is adequate segregation of duties in place, as Capita process the payments and the councils' revenues and benefits team review and authorise the payment runs.

5.3.2 A review of the returned cheques process identified that a stop is placed when the cheque is not physically held and marked as void. Payments are re-issued where necessary once the stop has been confirmed by the bank. Internal audit is satisfied that all returned and replacement cheques are dealt with appropriately with a satisfactory audit trail retained in the respective SODC and VWHDC benefits systems.

5.3.3 Area assurance: Full
No recommendations have been made as a result of our work in this area.

5.4 **Benefits overpayment recovery**

5.4.1 Overpayments may occur in cases where changes of circumstances that affect the previously awarded payments are not declared to the council in a timely manner by the claimant. At the time of the audit review (February 2020), there were 4,499 (2,290 SODC and 2,209 VWHDC) outstanding overpayment invoices. A sample of 40 (20 SODC and 20 VWHDC) overpayment invoices was selected to ensure recovery action had progressed in accordance with the timescales set out in the Corporate Debt Recovery Strategy (CDRS). Review found that 15 (11 SODC and four VWHDC) invoices had not had recovery action taken in accordance with the councils' corporate debt recovery strategy. Of the 40 overpayment invoices selected, eight (six SODC and two VWHDC) were referred to the legal team for possible prosecution action. Review of the eight invoices confirmed that appropriate legal action was taken to try and recoup the outstanding overpayment debt.

5.4.2 Not all debts are recoverable, e.g. low values which are uneconomical to pursue, and therefore may need to be written off. In 2019/2020 to date (February 2020), there were 267 (140 SODC and 127 VWHDC) overpayment invoices written off. A sample of 40 (20 SODC and 20

VWHDC) invoices were selected and review confirmed that all write offs were:

- reviewed by the councils' revenues and benefits team;
- authorised appropriately, in line with the councils' constitution.

5.4.3 Monthly reconciliations of overpayment invoices that have been written off by Capita in the Advantage system are performed, once the councils authorise the write off. Review of the reconciliation process identified no issues.

5.4.4 Area assurance: Limited
One recommendation has been made as a result of our work in this area (Rec 3).

5.5 **Housing benefits subsidy claim**

5.5.1 The councils claim government subsidy to cover eligible benefit expenditure. In 2018/2019, the councils' external auditors (Ernst and Young) gave both SODC and VWHDC an unqualified opinion on their subsidy return. As Ernst and Young review the benefit claims for subsidy purposes as prescribed by the Department of Works and Pensions (DWP), no additional checks have been made as a part of this review.

5.5.2 Area assurance: Full
No recommendations have been made as a result of our work in this area.

5.6 **Prevent and detect fraud**

5.6.1 The councils follow the guidance provided in the following policies regarding detection and referral of fraud:

- joint anti-fraud and corruption policy;
- joint anti-fraud and corruption policy response plan;
- joint prosecutions and sanctions policy (specifically for benefit fraud).

Internal audit reviewed each policy and concluded they are adequately detailed and provide details of the key decision makers and tools available for council prosecutions.

5.6.2 There are three ways the councils' fraud and investigation team are notified of any suspected fraud by:

- National Fraud Initiative (NFI) database;
- Capita benefits assessors; or
- members of the public.

Both councils also publicise the council's stance against benefit fraud and encourage members of the public to report any suspected fraud on their respective websites. Capita benefits assessors refer any potential fraud to the fraud and investigation team either via I@W (electronic document and records management system) or email for further scrutiny. It is noted that housing benefit fraud is investigated by DWP's single fraud investigation service; however, are routed through the councils' fraud and investigation team and checked for any potential work regarding CTRS prior to passing the referral to the DWP.

5.6.3 A data sharing agreement is in place between DWP and the councils in Oxfordshire, and any information required is requested by completing a local authority information exchange form, if DWP require information, or a single fraud investigation referral, if the councils require information from DWP. Quarterly liaison meetings also take place between DWP and the Oxfordshire councils, with the last one being 14 January 2020.

5.6.4 Area assurance: Full
No recommendations have been made as a result of our work in this area.

5.7 **Performance**

5.7.1 The councils send their performance statistics (i.e. performance indicators that measure the speed and accuracy with which applications are administered) obtained from the Advantage system and report these monthly to the DWP. The DWP also publish the councils' performance statistics (e.g. speed of processing) on their website. From 1 August 2016, Capita provide the benefits service under the 5CP contract and there is an output specification, key performance indicators (KPI's) and performance indicators (PI) for the services within the contract. These targets are a part of managing the contract with Capita who provide benefits services to both SODC and VWHDC. At the time of audit (March 2020), the most recent report was for January 2020. Review of the performance report found that there is no explanation for any variances occurred.

5.7.2 Area assurance: Substantial
One previous recommendation has been restated as a result of our work (Rec 2).

6. ACKNOWLEDGEMENTS

6.1 Internal audit would like to take this opportunity to thank all staff involved for their assistance with the audit.

7. CATEGORISATION OF RECOMMENDATIONS

7.1 To assist management in using our reports, we have categorised our recommendations according to their level of priority as follows:

High risk	Fundamental control weakness for senior management action	**Rec 3**
Medium risk	Other control weakness for local management action	
Low risk	Recommended best practice to improve overall control	**Recs 1 and 2**

OBSERVATIONS AND RECOMMENDATIONS

PREVIOUS RECOMMENDATIONS RESTATED

1. GDPR compliance (Low Risk)

Rationale	Recommendation	Responsibility
Best Practice Application forms and website information for DHP, housing benefits and CTRS contain, or link to, GDPR information and privacy notices. Findings There is no reference to data protection privacy notices or the councils' data protection information on the following: • DHP application form; • Council webpages for applying for DHP or housing benefits and CTRS Risk Non-compliance to GDPR legislation, which could result in fines and reputational damage.	Review and update housing benefits/CTRS and DHP information on the councils' webpages and on application forms to include GDPR information, e.g. privacy notices.	Revenues and Benefits Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed** The requirements are confusing. Although there are general statements on the websites the exact requirements are being determined by the 5C's forum. As soon as requirements are specified, I will ensure they are implemented. Management response: Revenues and Benefits Manager		30 September 2020

2. Performance reports (Low Risk)

Rationale	Recommendation	Responsibility
Best Practice The councils receive regular reports on all agreed performance indicators with explanations of variances. Findings A monthly spreadsheet is provided by Capita recording performance for housing benefit and CTRS as well as council tax and NNDR. However, review of January 2020 spreadsheet found that explanation of variances is not recorded. Risk Areas of underperformance may remain unidentified and uncorrected.	Monthly performance reports should include explanations of variances and include all required KPI and PI figures.	Revenues and Benefits Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed in Principle** Unfortunately, our councils are now part of the 5C's arrangements, and the performance reports are produced in accordance with those governing requirements. Saying that, our councils have previously		30 September 2020

agreed a shortened bespoke report similar to what we received in the past. This would provide commentary on performance and I will ask for it to be produced again (as it has lapsed). It should be noted however that commentary is provided our councils Board Report in respect of collections and benefit processing. Management response: Revenues and Benefits Manager	

BENEFITS OVERPAYMENT RECOVERY

3. Recovery process (High Risk)

Rationale	Recommendation	Responsibility
Best Practice All overpayments are progressed through the recovery process in a timely and efficient manner. Findings In 2019/2020 to date (January 2020), there were 4,499 (2,290 SODC and 2,209 VWHDC) outstanding housing benefits overpayment invoices totalling £5,082,457 (£2,622,227.97 SODC & £2,460,229 VWHDC). A sample of 40 (20 SODC and 20 VWHDC) outstanding housing benefits overpayment invoices was selected using both statistical and non-statistical sampling methods. Review found that 15 (11 SODC and four VWHDC) overpayment invoices had not been progressed through the recovery process efficiently and in line with the corporate debt recovery strategy. The total value of the 15 errors identified is £153,132 (£120,028 SODC and £33,104 VWHDC). Due to the high error rate (37.5%) identified in both the SODC (55%) and VWHDC (20%) overpayment samples, an additional sample of 20 (10 SODC and 10 VWHDC) overpayments were tested. A statistical sampling method was used to select the additional sample. Based on our review of the additional overpayments, no issues were identified. Risk If overpayments are not reviewed and progressed through the recovery process in a timely and efficient manner, it may prove difficult to recover the overpayment resulting in writing off the account.	A reminder should be sent to Capita benefits team to attempt to recover overpayments in line with the councils' corporate debt recovery strategy.	Revenues and Benefits Manager
Management Response		**Implementation Due Date**
Recommendation is **Agreed**		31 October 2020

It is fair to say that the from the commencement of the 5C's contract, it was immediately evident that the new 5C's overpayment recovery function was in need of a review of resourcing and processes as it was not conducive for the "maximisation of overpayment income" as specified in the contract. However, in the last year, as far as South and Vale is concerned, we have seen a significant improvement in recovery rate performance, which has been confirmed by DWP statistics. We have collected more than we have raised, which is probably down to a combination of increased recovery action by the team (a combination of the new and committed Capita team and our own expert legal services and we use every recovery tool allowed) and fewer overpayments being created as Universal Credit kicks in. We need to sustain and even try to improve on this, so in the next few months (COVID allowing) we will consider the best way forward, including an independent review of the caseload. Management response: Revenues and Benefits Manager	

3. Elections and Election Payments 2019/2020 – Follow up Review

MANAGEMENT SUMMARY

1. INTRODUCTION

1.1 This report details the findings from internal audit's follow-up review of elections and election payments 2019/2020. The original fieldwork was undertaken in November 2019 and the final report was issued in December 2019. Follow-up work has been undertaken in accordance with the 2019/2020 audit plan agreed with the joint audit and governance committee of South Oxfordshire District Council (SODC) and Vale of White Horse District Council (VWHDC), to ensure that the agreed recommendations have been implemented within the timescales provided.

2. INITIAL AUDIT FINDINGS

2.1 The final report made five recommendations, and all were agreed. A limited assurance level opinion was issued.

3. FOLLOW UP MAIN FINDINGS

3.1 The review found that all five recommendations have been implemented.

4. ACKNOWLEDGEMENTS

4.1 Internal audit would like to take this opportunity to thank all staff involved for their assistance with the follow-up audit.

FOLLOW-UP OBSERVATIONS

ROLES AND RESPONSIBILITIES

1. Online training **(Medium Risk)**

Rationale	Recommendation	Responsibility
Best Practice Presiding officers, poll clerks and polling station inspectors complete the online training, prior to the elections. Findings The following elections staff worked at the May 2019 elections: *District and parish councils' elections* • 203 (108 SODC and 95 VWHDC) presiding officers; • 276 (147 SODC and 129 VWHDC) poll clerks; • 14 (7 SODC and 7 VWHDC) polling station inspectors.	a) A reminder notice should be issued to presiding officers and poll clerks who have not completed the mandatory online training prior to the elections, reminding them of the requirement to do so in order to understand their duties. b) The elections team should perform a review of the online training records and decide whether to consider appointing staff for election duties in the future.	Electoral Services Team Leader

European parliament election • 206 presiding officers; • 281 poll clerks; • 14 polling station inspectors. From review of all presiding officers, poll clerks and polling station inspectors who worked at both elections, internal audit found that 11 (two SODC presiding officers, three SODC poll clerks, one VWHDC presiding officer and five VWHDC poll clerks) elections staff did not complete the online training. Risk If presiding officers, poll clerks and polling station inspectors do not complete the online training, there is a risk that staff do not carry out their duties appropriately, which may result in errors and reputational damage.		
Management Response		**Implementation Due Date**
Recommendation is **Agreed** This will be implemented for the Police and Crime Commissioner election in May 2020. Management response: Electoral Services Team Leader		31 May 2020
Follow-up observations		
a) The appointment letter for both poll clerk and presiding officers both state that training is required to undertake their role. The elections team also sends out reminder emails to election staff that have not undertaken the training. Evidence has been provided and filed. b) The electoral services team leader stated that a review was undertaken and found no evidence of repeat offenders of not undertaking the required training.		**Implemented**

SCHEDULE OF FEES

2. Staff payment review (High Risk)

Rationale	Recommendation	Responsibility
Best Practice Elections staff payments are calculated correctly and in line with the agreed scale of fees. Findings In October 2018, both SODC and VWHDC Council meetings approved the elections scale of fees. The scale of fees state that staff working on the count are paid: • for the first hour; • for each half hour thereafter or part thereof. The following elections staff worked at the May 2019 counts:	A reminder should be sent to the elections team members to thoroughly review the payroll records to ensure that the amounts due to be paid to elections staff are accurately calculated and in line with the agreed scale of fees, prior to it being sent to Selima for payment.	Democratic Services Manager

District and parish councils' elections • 160 (80 SODC and 80 VWHDC) count assistants; • 40 (20 SODC and 20 VWHDC) count supervisors; • 164 (81 SODC and 83 VWHDC) overnight count assistants; • 42 (21 SODC and 21 VWHDC) overnight count supervisors. *European parliament election* • 146 count assistants; • 21 count supervisors; • 149 verification assistants. The approved scale of fees states that staff working on the count are paid for the first hour and for each half hour thereafter or part thereof. A sample of 22 (eight SODC, eight VWHDC and six European) elections staff at the count was selected and review found that 19 staff were paid incorrectly (12 were overpaid and seven were underpaid) and not in line with the agreed scale of fees. Risk If elections staff payments are not calculated correctly, there is a risk of overpayment of staff resulting in a financial loss to the councils.		
Management Response		**Implementation Due Date**
Recommendation is **Agreed** The scales of fees and charges agreed by the councils do not apply to the Parliamentary elections in December 2019 or the Police and Crime commissioner elections in May 2020, but the same principle will be applied to the fee structure agreed by the Acting Returning Officer/Local Returning Officer. Management response: Democratic Services Manager		31 January 2020
Follow-up observations		
The elections team leader stated that review of payroll was undertaken for the staff that worked in the December 2019 general elections. Review of five elections staff pay confirmed that staff working on the elections were correctly paid.		**Implemented**

3. Signing in and out at the count (Low Risk)

Rationale	Recommendation	Responsibility
Best Practice Elections staff working at the count as either an assistant, supervisor or verifier, fill in the signing in and out sheet. Findings A sample of 22 (eight SODC, eight VWHDC and six European) elections staff at the count was selected and review	A notice should be issued to all elections staff on the count, as either an assistant, supervisor or verifier, to fill in the signing in and out sheet.	Electoral Services Team Leader

found that one overnight supervisor did not sign in or out sheet and was paid for nine hours of work. It is noted that the individual did confirm their hours via email. Also, review of the signing in and out sheets found that the sheets were filled in by the same officer and not by the individuals working at the count. Risk If elections staff do not fill in the signing in and out sheet, there is a risk of them either not being paid or being paid incorrectly.		
Management Response		**Implementation Due Date**
Recommendation is **Agreed** Count supervisors are instructed to ensure that this happens, and this will be reinforced. Management response: Democratic Services Manager		31 December 2019
Follow-up observations		
Internal audit obtained copies of the election staff signing in records for the general elections, which were held on 12 December 2019. Review of the records confirmed that election staff on the count are now signing in and out.		**Implemented**

CHECKING, AUTHORISING AND ELECTION PAYMENTS

4. Returning of acceptance and staff payment forms (Low Risk)

Rationale	Recommendation	Responsibility
Best Practice Elections staff complete and return both acceptance of appointment (Form A) staff payment (Form B) forms prior to working on the elections. Findings At both May 2019 elections, there were: • 505 elections staff - SODC district and parish elections; • 479 elections staff - VWHDC district and parish elections; • 853 elections staff - European parliament elections. A sample of 33 (11 SODC, 12 VWHDC and ten European) found that three European election staff did not complete and return either Form A - acceptance of appointment and Form B - staff payment and were paid for undertaking their role. Risk If elections staff do not complete and return Form A, there is a risk of the	A reminder should be sent to all election staff members to complete and return both Form A - acceptance of appointment and Form B - staff payment.	Electoral Services Team Leader

councils not receiving any formal acceptance to undertake the role resulting in a possible no show to undertake the role. If elections staff do not complete and return Form B, there is a risk of staff being incorrectly taxed.		
Management Response		**Implementation Due Date**
Recommendation is **Agreed** This will be done as far as possible, but Form A is not always achievable for staff appointed at short notice e.g. to replace staff who withdraw Management response: Democratic Services Manager		31 May 2020
Follow-up observations		
Internal audit obtained evidence of reminder emails being sent out to elections staff when not returned to the councils.		**Implemented**

POST-ELECTION PERFORMANCE REVIEW

5. Post-election action plan (Medium Risk)

Rationale	Recommendation	Responsibility
Best Practice An action plan is in place and followed to rectify any issues identified following the previous election. Findings Post-election reviews of both the district and parish councils' elections and the European parliament election were undertaken by the elections team, project team and the consultant from the Association of Electoral Administrators and issues were identified. In October 2019, a report went to both SODC and VWHDC's Community Governance and Electoral Issues Committee and key actions were noted in the report. An action plan was developed by the external consultant and at the time of the audit (October 2019) the elections team were working through the actions. However, an action plan has not been developed regarding the issues identified in the post-election reviews undertaken by both the elections team and the project team; nor has an action plan been developed regarding to the key actions noted in the report to the committee. Risk If an action plan is not in place to rectify any issues identified in the May 2019	An action plan with implementation target dates should be developed to ensure that any issues identified from the May 2019 elections in the post-election reviews are in place prior to the next elections.	Electoral Services Team Leader

elections, there is a risk that the councils will not learn from any mistakes made resulting in the same error being made in the next elections.		
Management Response		**Implementation Due Date**
Recommendation is **Agreed** This will be signed off at the Gateway 3 project closure and delivery review report. Management response: Democratic Services Manager		31 March 2020
Follow-up observations		
Issues identified during the elections post review are now part of the election team's action plan. Review of the action plan found that actions were completed and implemented at the December 2019 general elections.		**Implemented**