Division(s): N/A

AUDIT and GOVERNANCE COMMITTEE – 5 January 2022

INTERNAL AUDIT 2021/22 PROGRESS REPORT

Report by the Director of Finance

RECOMMENDATION

1. **The committee is RECOMMENDED to**

   a) **Note the progress with the 2021/22 Internal Audit Plan and the outcome of the completed audits.**
   b) **Note the Blue Badge Enforcement Strategy.**

EXECUTIVE SUMMARY

2. This report provides an update on the Internal Audit Service, including resources, completed and planned audits.

3. The report includes the Executive Summaries from the individual Internal Audit reports finalised since the last report to the September 2021 Committee. Since the last update, there have been no further red reports issued.

PROGRESS REPORT:

RESOURCES

4. A full update on resources was made to the Audit and Governance Committee in June 2021 as part of the Internal Audit Strategy and Plan for 2021/22. There are currently no vacancies within Internal Audit / Counter Fraud.

5. One of the new Senior Auditors who commenced in November 2020, went on maternity leave from the middle of June 2021. She is due back in quarter 4. We have arranged a temporary resource to cover some of the work, he will be with us from the beginning of January to the end of March 2022.

6. We are continuing to support team members to compete both the Chartered Internal Audit Qualification and the Certified Internal Audit Qualification. Two of the Senior Auditors have recently passed one of the Certified Internal Audit exams, their studies are continuing. The Audit Manager and other Senior Auditor are due to sit their final exam of the Chartered level in the new year. The Assistant Auditor and Counter Fraud Intelligence Officer are undertaking apprenticeships.

2021/22 INTERNAL AUDIT PLAN - PROGRESS REPORT

7. The 2021/22 Internal Audit Plan, which was agreed at the June 2021 Audit & Governance Committee, is attached as Appendix 1 to this report. This shows current progress with each audit and any amendments made to the plan. The plan and plan progress is reviewed quarterly with the individual directorate leadership teams.

8. There have been 7 audits concluded since the last update, summaries of findings and current status of management actions are detailed in Appendix 2. The completed audits are as follows:

FINAL Reports:

Directorate	**2021/22 Audits**	**Opinion**
Customers, OD & Resources – IT	IT Business as usual Change Management 2021/22	Amber
Childrens	Supported Families – Claim 2 – Claim certified	N/A
Customers, OD & Resources – IT	IT Software Asset Management 2021/22	Green
Customers, OD & Resources – HR	IR35 2021/22	Green
CDAI	GDPR 2021/22	Amber
Children's	Stage 2 IT audit of Children's Education System Implementation 2021/22	Green
Customers, OD & Resources – Finance / IT & CDAI - Information Governance	PCI-DSS 2021/22	Green
Corporate / Cross cutting	Fleet Management 2021/22	Amber

The following **grant certification** work has been completed since the last report to A&G:

- Local Transport Capital Funding (included Integrated Highways Maintenance Grant and Pothole and Challenge Fund) – certified end of Sept 21.
- Additional dedicated home to school and college transport grant.

  Tranches 5 & 6 - certified end of Sept 21

  Tranche 7 – certified end of Oct 21
- OCC Disabled Facilities Grant – certified end of Oct 21
- Bus Subsidy Grant – certified Nov 21

PERFORMANCE

9. The following performance indicators are monitored on a monthly basis.

Performance Measure	Target	% Performance Achieved for 21/22 audits (as at 01/09/21)	Comments
Elapsed time between start of the audit (opening meeting) and Exit Meeting.	Target date agreed for each assignment by the Audit manager, stated on Terms of Reference, but should be no more than 3 X the total audit assignment days (excepting annual leave etc)	67%	Previously reported year-end figures: 2020/21 50% 2019/20 61% 2018/19 69%
Elapsed Time for completion of audit work (exit meeting) to issue of draft report.	15 days	92%	Previously reported year-end figures: 2020/21 88% 2019/20 74% 2018/19 82%
Elapsed Time between issue of Draft report and issue of Final Report.	15 days	55%	Previously reported year-end figures: 2020/21 80% 2019/20 74% 2018/19 85%

The other performance indicators are:

- % of 2021/22 planned audit activity completed by 30 April 2022 - reported at year end.

- % of management actions implemented (as at 07/12/21) – 73%. Of the remaining there are 4% of actions that are overdue, 6% partially implemented and 17% of actions not yet due.
  (At September 2021 A&G Committee the figures reported were 72% implemented, 3% overdue, 9% partially implemented and 16% not yet due)

- Extended Management Team satisfaction with internal audit work - reported at year end.

COUNTER-FRAUD

10. The next counter fraud update to Audit & Governance Committee is scheduled for March 2022.

11. At the November 2021 A&G meeting, we reported that we were in the process of drafting the Blue Badge Enforcement Strategy. This work is now complete, and the Strategy is included as Annex 3 to this report. The Strategy was written by the Counter Fraud team in consultation with colleagues across the directorates, including Highways, Customer Services, Adults and Childrens, Finance and the cabinet members for Finance and Highways Management.

12. The Blue Badge Enforcement Strategy sets out Oxfordshire County Council's responsibility for administration and enforcement of the Blue Badge Scheme and provides a framework for us to deal with Blue Badge misuse.

SARAH COX
Chief Internal Auditor

Background papers: None.
Contact Officer: Sarah Cox sarah.cox@oxfordshire.gov.uk

APPENDIX 1 - 2021/22 INTERNAL AUDIT PLAN - PROGRESS REPORT

Audit	Planned Qtr Start	Status as at 7/12/21	Conclusion
Corporate / Cross Cutting			
Provision Cycle - Prepare, Tender and Implement.	Q3	Fieldwork	
Provision Cycle - Manage & Review	Q3	Fieldwork	
Childrens			
Children's Payments via ContrOCC / LCS recording	Q3/Q4	Not started	
Childrens Education System – Implementation of New Council IT System	Q1-Q4	Phase 1 IT controls – completed (Green) Phase 2 IT controls – completed (Green) Phase 3 and 4 IT controls – Q4 Operational processes – not started.	Summary of overall conclusion to be presented at end of year.
Supporting Families	Q1-Q4	Claim 1 – Certified Claim 2 – Certified Claim 3 – not started	-
Family Solutions Plus	Q3/Q4	Not started	
SEND	Q3	Deferred to Q1 of 2022/23 internal audit plan – see plan amendments below.	-
Education Safeguarding	Q3	Scoping undertaken Q1 – deferred to Q3/Q4 at request of service Fieldwork now started	
Addition to Plan: Five Acres Primary School – Financial Management Audit	Q3	Fieldwork completed	

Adults & Housing			
Direct Payments – Follow Up	Q4	Scoping	
Payments to Providers	Q3/Q4	Due to start Q3 – moved to Q4 due to IA team member sickness absence	
Client Charging	Q1	Final Report	Amber
Money Management	Q3	Fieldwork	
Supplier Business Continuity	Q2/Q3	Removed from 2021/22 plan – see plan amendments below	-
Customers, OD & Resources – HR			
Well-being / Sickness Management	Q1/Q2	Fieldwork	
IR35 (off-payroll rules)	Q1/Q2	Final Report	Green
Customers, OD & Resources – Finance			
Treasury Management	Q4	Scoping	
Growth Board – Accountable Body Role	Q1/Q2	Fieldwork	
Pensions Administration	Q4	Fieldwork complete	
Customers, OD & Resources – Finance / IT			
Payment Card Industry Data Security Standard (PCI-DSS)	Q1	Final Report	Green
Customers, OD & Resources – IT			
Cyber Security	Q1	Final Report	Amber
IT “business as usual” Change Management	Q2	Final Report	Amber
Software Asset Management	Q3	Final Report	Green
Data Centre	Q4	Scoping – agreed Jan start	
Customers, OD & Resources – Cultural Services			
Music Service Follow Up	Q4	Not started	
CDAI – Fire & Rescue & CODR – HR / Finance			
Gartan Payroll & HR Processes	Q2	Draft Report	
CDAI			
GDPR	Q2	Final Report	Amber
Property / Facilities Management	Q4	Not started	

CDAI / Corporate / Cross Cutting			
Fleet Management – Compliance	Q2	Final Report	Amber
Environment & Place / CODR – Finance			
Capital Programme - Major Infrastructure	Q3	Removed from 2021/22 plan – see plan amendments below	-
Capital Programme - Highways Asset Management	Q3	Removed from 2021/22 plan – see plan amendments below	-
Environment & Place			
Highways Contract Management	Q2/Q3	Not started – service requested Q4 start	
S106 – Spend	Q1/Q2	Draft Report	
Various / Corporate / Cross Cutting			
Combined Audit & Counter Fraud Reviews	Q1-Q4	-	
Covid-19 Funding / Payments	Q1-Q4	-	
Grants	Q1-Q4	• Building Digital UK – certified end of June 21 • Local Transport Capital Funding (included Integrated Highways Maintenance Grant and Pothole and Challenge Fund) – certified end of Sept 21. • Additional dedicated home to school and college transport grant.	

		Tranches 5 & 6 - certified end of Sept 21 Tranche 7 – certified end of Oct 21 • OCC Disabled Facilities Grant – certified end of Oct 21 • Bus Subsidy Grant – certified Nov 21	

Amendments to OCC Internal Audit Plan 2021/22

Directorate	**Audit**	**Reason for amendment**
Childrens	Five Acres Primary School	Addition to plan Requested by Childrens Directorate – financial management audit of the school.
Childrens	SEND	Deferred to Q1 of 2022/23 plan. The audit was planned for Q4 of 2021/22, but has been deferred by a couple of months, recognising the significant work currently being undertaken in relation to the consultation on the SEND Strategy. Significant progress has been reported on the implementation of actions agreed in the

		previous audit, with the majority implemented and good progress with the remaining actions.
Adults	Supplier Business Continuity	Removed from plan as separate audit. This will be covered under the wider audit of Provision Cycle – Manage and Review.
Environment & Place / CODR – Finance	Capital Programme - Major Infrastructure	Deferred A fundamental review of capital governance is underway. This audit has therefore been removed from the 2021/22 Internal Audit Plan and will be considered again during audit planning for 2022/23. – Agreed with Director of Finance.
Environment & Place / CODR – Finance	Capital Programme - Highways Asset Management	Deferred A fundamental review of capital governance is underway. This audit has therefore been removed from the 2021/22 Internal Audit Plan and will be considered again during audit planning for 2022/23. – Agreed with Director of Finance.

APPENDIX 2 - EXECUTIVE SUMMARIES OF COMPLETED AUDITS

Summary of Completed Audits 2021/22 since last reported to Audit & Governance Committee September 2021

IT Business as usual Change Management 2021/22

Overall conclusion on the system of internal control being maintained	**A**

RISK AREAS	AREA CONCLUSION	No of Priority 1 Management Actions	No of Priority 2 Management Actions
IT Service Policy and Process	**A**	**0**	**1**
Change Management Approach	**A**	**0**	**3**
Emergency Changes	**G**	**0**	**0**
Testing	**A**	**0**	**1**
Documentation	**G**	**0**	**0**
		0	**5**

Opinion: Amber		
Total: 5	Priority 1 = 0	Priority 2 = 5
Current Status:		
Implemented	1	
Due not yet actioned	2	
Partially complete	1	
Not yet Due	1	

IT business as usual changes are managed on the new IT service management tool and are subject to a formal review and approval process, in accordance with good practice and the ITIL (Information Technology Infrastructure Library) framework. IT Services have a documented policy on Change Management. It is from 2012 and requires updating to reflect current standards and processes, following which it will need to be communicated across the service to ensure all relevant staff are aware of requirements.

All IT business as usual changes are logged on the IT service management tool and reviewed and approved by a Change Advisory Board (CAB). Various details

have to be logged for each new change request, including the priority of the change. A review of how priority is determined found that it is not based on any formal assessment, such as 'impact' and 'urgency', and hence there is a risk that changes are not prioritised correctly or consistently. There are a list of standard changes, which are pre-approved and it was confirmed that they have been subject to recent review. In addition to the CAB, there is a Change Review Board (CRB) who look at all completed changes to ensure all relevant tasks have been undertaken. The responsibilities of the CRB are not documented and hence it is unclear what specific tasks they should perform. For example, we were informed that they should look at any changes that are backed out and found that this is not undertaken. There is also no formal management level reporting on the change management function to confirm it is performing as required.

Emergency changes are covered within the IT Change Management Policy and are generally limited to changes that need to be made urgently to address a major incident or a zero day security vulnerability. All such changes are logged on the IT service management tool and have to be approved by an Emergency CAB. No significant risk issues were identified in this area.

The requirement to test changes, where relevant and applicable, is not documented within the Change Management Policy and there is no facility within the IT service management tool to add a test plan for all proposed changes. This presents a risk that changes are not adequately tested and could lead to IT incidents or problems after a change is made.

The documentation that needs to be updated following a change is identified when the change request is logged and is followed up by the CRB. No significant risk issues were identified in this area.

Supported Families October 2021 Claim

Introduction

The current claim consists of 206 families for **Significant & Sustained Progress (SSP).** This brings the total for the year to 360 families so far.

The audit of the previous claim (June 2021) identified no issues or management actions, owing to the previous improvements to the process for identifying duplicate claims and updates to the Think Family Outcome Plan. All previous actions from previous audits have been implemented.

Overall Conclusion

The audit noted the improvements in the internal processes for data checking and validation made following previous claims have remained effective. Testing for duplicates found no families that have previously been claimed for, and no issues were identified with the eligibility or sustained progress of the families sampled.

Due to satisfactory responses having been received for all queries raised by Internal Audit, this claim can be signed off for submission.

As such, no audit findings or management actions were required.

IT Software Asset Management 2021/22

Overall conclusion on the system of internal control being maintained	G

RISK AREAS	AREA CONCLUSION	No of Priority 1 Management Actions	No of Priority 2 Management Actions
IT Policy and Procedures	A	0	1
Software Procurement	G	0	0
Software Inventory and License Management	G	0	1
Software Installations	G	0	0
		0	2

Opinion: Green		
Total: 2	Priority 1 = 0	Priority 2 = 2
Current Status:		
Implemented	0	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	2	

Software Asset Management (SAM) refers to the act of controlling and managing software assets to better support and further organisational goals, as well as managing costs and risks. The audit has identified a strong system of controls in operation. There are defined responsibilities for managing computer software within IT Services and an ICT Software Policy is documented and published on the Intranet. A review of the policy found that it missed its annual review in 2019 and requires updating as it is shown as being owned by the Information Management team, from when they were part of IT Services, and they have no operational responsibility for managing computer software. The policy covers areas such as software procurement and installation but does not highlight the need for software audits and license reconciliations, which is an area that needs to be improved as detailed below. The risks of downloading computer software are covered within the ICT Software Policy and also the Acceptable Use Policy.

Software procurement procedures are in place and require all requests for new computer software to be logged and managed on the IT service management system. All requests have to be supported by a brief business case/justification and require line manager approval. We sample tested five recent requests for new computer software and confirmed these controls to be working effectively. If the

request is for non-standard software, it is passed to the IT Customer Engagement Team to follow-up with the relevant service area. Microsoft software is the biggest software expenditure and it is procured from a supplier who was selected following a competitive tender exercise. The current agreement runs until February 2022 and IT Services have started to work on a new tender. For non-Microsoft software, three quotes are always requested where possible and this was confirmed by our testing. When processing requests for new computer software, the IT Customer Request Team will look to see if an existing license can be re-allocated rather than buy a new one.

IT Services maintain a software inventory which has details of all software that has been procured and the relevant purchase order number and/or software license key. Our sample testing of recently procured software confirmed that inventory details are maintained up-to-date. The SCCM (System Center Configuration Manager) tool has details of all computer software installed on clients and this information is updated on a weekly basis. The number of licenses available for Microsoft 365 is monitored on a daily basis to ensure it is sufficient to cover all new starters. The number of AutoCAD users was also confirmed for licensing purposes when the software license was renewed earlier in the year. However, there has been no wider reconciliation of all software installed against licenses to ensure there is no unlicensed software in use, although our sample testing of a small number of software products (Adobe Acrobat, Visio Standard, Duxbury Braille Translator and ClaroRead Professional) confirmed that there are sufficient licenses for the software installed.

The ability to install software is limited to designated users in IT Services and where possible software is packaged and deployed using SCCM. No risk issues were identified in this area.

IR35 2021/22

Overall conclusion on the system of internal control being maintained	**G**

RISK AREAS	AREA CONCLUSION	No of Priority 1 Management Actions	No of Priority 2 Management Actions
Policies and Procedures	**G**	**0**	**1**
Roles and Responsibilities	**G**	**0**	**0**
IR35 Processes	**G**	**0**	**1**
		0	**2**

Opinion: Green		
Total: 2	Priority 1 = 0	Priority 2 = 2
Current Status:		
Implemented	1	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	1	

Changes to IR35 legislation came into effect in April 2021. These changes included the requirement to re-assess temporary roles once filled and communicate the results of that assessment to the worker. Prior to the IR35 legislative changes coming into effect, the Resourcing Team reviewed processes and arrangements for assessment and communication of IR35 status for temporary workers employed via the Council's temporary worker Contractor. There were also some investigations completed by the Team to review where there could be historic temporary contracting arrangements within the Council which could also have IR35 implications, outside of the arrangements with the current Contractor.

The audit found that there is clear and comprehensive guidance in place for managers on the process for the employment of temporary staff via the Council's temporary worker Contractor which includes guidance on IR35 processes and considerations. It was also noted that team processes and guidance have been reviewed and refreshed within the Resourcing Team with process flow documents now being finalised and rolled out. Roles and responsibilities relating to IR35 considerations when using the Council's temporary worker Contractor were also found to be clearly defined and communicated.

At the time of audit testing, intranet guidance for the engagement of temporary workers outside of the arrangements with the Council's temporary worker Contractor was found to be less clear with some types of role where IR35 needs to be assessed not making clear reference to the required IR35 processes. Roles and responsibilities were not as clearly defined. Whilst it is acknowledged that there should be minimal cases where temporary workers are recruited outside of the arrangements with the temporary worker Contractor, the same IR35 processes apply. Following discussions during the audit, this guidance has been reviewed and simplified. Managers are now routed back to the Resourcing Team which will help to ensure that the correct temporary recruitment and IR35 assessment processes are followed.

Sample testing on the IR35 assessment process found processes for assessing and communicating IR35 status to be operating effectively. There is a clear process in place for the assessment of new roles, in accordance with IR35 legislation, prior to recruitment, review of that role and communication of the decision on IR35 status following the temporary role being filled. As noted above, managers wanting to fill temporary vacancies outside of the standard arrangements with the temporary worker Contractor are now directed, by the intranet guidance, back to the Resourcing Team. There are also processes in place to route temporary recruitments outside of the Council's temporary recruitment contract back through to the Resourcing Team (for example via the Procurement Team) so that they are able to ensure that the correct recruitment and IR35 processes are followed.

From the work undertaken within the Resourcing Team, in preparation for the IR35 legislative changes, to identify historic arrangements where there may be roles requiring assessment under IR35 legislation, it was noted that there are a couple of areas where processes are being reviewed and confirmed to ensure that the correct temporary recruitment and IR35 assessment processes are followed going forward.

GDPR 2021/22

Overall conclusion on the system of internal control being maintained	**A**

RISK AREAS	AREA CONCLUSION	No of Priority 1 Management Actions	No of Priority 2 Management Actions
Corporate Policy	**A**	**0**	**2**
Governance Structure	**A**	**0**	**4**
Information Audit	**R**	**1**	**1**
Privacy Notice	**A**	**0**	**2**
Data Subject Rights	**G**	**0**	**0**
Data Breaches	**G**	**0**	**0**
Privacy by Design	**A**	**0**	**2**
		1	**11**

Opinion: Amber		
Total: 12	Priority 1 = 1	Priority 2 = 11
Current Status:		
Implemented	0	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	12	

The UK GDPR (General Data Protection Regulation) 2021 and the Data Protection Act 2018 collectively set out the UK's data protection regime. The UK GDPR incorporates the EU GDPR regulation into UK law, following withdrawal from the European Union. There is a good governance structure in place within Oxfordshire County Council for the management and oversight of GDPR compliance. This

includes a corporate Information Governance Group (IGG), which reports to an Information Governance Board (IGB). There is a dedicated Information Management team and a documented Data Protection Policy which sets out the organisation's approach to data protection compliance. The Council has a current data protection registration which expires in November 2021.

A review of the corporate policy and structure for data protection identified the following areas for improvement:

- Whilst the Data Protection Policy is reviewed annually, there is no evidence of it being formally approved.
- A corporate retention schedule is published on the Intranet and defines retention periods for records and documents. The Information Management team review retention periods with service areas as part of the annual review of Information Asset Register's (IAR's) but there is no assurance mechanism in place to confirm that data is not held beyond its agreed retention period.
- There is a 'DPO Plan 2019/20' which has a list of actions to help ensure the Council complies with its data protection obligations. There has been no recent review of the plan and all the actions are shown as being outstanding.
- Membership of the IGG would benefit from being reviewed to ensure all directorates/critical service areas that process personal data are adequately represented.
- The IGB should meet at the agreed interval and a formal record should be maintained of all IGB and IGG meetings.

OCC require all staff to undertake annual training on data protection. There is a mandatory data protection essentials e-learning training course and our sample testing found that 70% of people last completed it in 2019 and hence may not have a current awareness of their data protection responsibilities. There is an outstanding management action from our previous GDPR audit in 2018/19 to address additional training requirements for members of the Information Management team. This is currently being progressed.

One of the key changes introduced by GDPR is the requirement to maintain records of all processing activities, which is important as it supports good data governance and helps demonstrate compliance with UK GDPR. Information Asset Registers (IAR's) are held as records of processing activities but we found they are incomplete and do not capture all relevant details. There is an outstanding action from our previous audit to complete data flow mapping to validate the IAR's. A review of the way in which 'consent' is used has not been performed since the implementation of GDPR in 2018 and hence there is a risk that new consents may not comply with GDPR standards.

Privacy notices need to be improved to ensure the individual's right to be informed about the use of their personal data is respected. The privacy notice on the corporate website is not sufficiently detailed. We also identified a number of paper forms that collect personal data that do not have a privacy notice or it does not meet GDPR standards. The same issues were reported in our previous GDPR audit.

There is a procedure for dealing with subject access requests and other information rights, which are managed by the Information Management team. All requests are logged and the authenticity of the requesting person is confirmed as part of the process. There are no significant risks in this area.

Security incident reporting procedures are in place and require all incidents to be reported to the IT service desk. All information related incidents, as opposed to IT/cyber incidents, are notified to the Information Management team for further review and investigation. All incidents and remedial actions are reported to IGG.

Data Protection Impact Assessments (DPIA's) are performed to help identify and minimise the data protection risks of a project. There is a comprehensive template available to support these reviews but the process for carrying them out is not documented and hence roles, responsibilities and sign-off requirements are unclear. Our sample testing of four recently completed DPIA's identified issues around the recording of DPO comments and one where the 'risks and issues' section had not been completed, which is a key part of the DPIA process.

There were 12 management actions agreed in the 2018/19 audit of GDPR, 10 of which have been closed by management on the basis of being implemented. Two actions are still outstanding relating to a review of IAR's and training for the Information Management team. A review of the 10 closed actions identified four that have not been fully implemented, which relate to a review of privacy notices on forms, compliance with data retention periods, a review of consent and the development of service specific privacy notices. These have been raised again in this report.

IT audit of Children's Education System Implementation - Stage 2

Overall conclusion on the system of internal control being maintained	**G**

Opinion: Green		
Total: 4	Priority 1 = 0	Priority 2 = 4
Current Status:		
Implemented	0	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	4	

Introduction

The audit is being undertaken in a number of stages throughout the year. Internal Audit is covering both assurance over the design of operational processes and controls for the new system and also key IT system processes and controls. This reports on the second stage review, which looked at System Security risks.

Overall Conclusion

Our overall conclusion is Green. This is based on the scope of the work undertaken relating to the consideration of the implementation of key system controls in relation to system security.

This stage review has focussed on Liquidlogic EYES (Early Years & Education Management System.) The Liquidlogic Integrated Finance Technology (LIFT) system was not reviewed as delivery from the supplier is behind schedule and hence work on system security has not yet started.

The EYES system will utilise Single Sign-On (SSO) and the majority of users will be authenticated based on their network credentials. A small number of users will have secondary accounts and they will have to login locally to EYES to access these accounts. These secondary accounts will be subject to the EYES password policy and we confirmed that a minimum password length is enforced, although there were no further details available on complexity requirements, expiry periods and account lockout policy. These areas should be confirmed to be in accordance with corporate password standards.

User access rights are being defined and will be formally signed off by service area leads. All access rights will be documented and we have highlighted the importance of ensuring this documentation is maintained after go-live to ensure the information is available to support subsequent reviews of user access rights.

System audit trail requirements were included in the specification of requirements but the functionality has not been reviewed to see how it works, what activity is being logged and how it can be reported on. This should be confirmed before go-live.

PCI-DSS 2021/22

Overall conclusion on the system of internal control being maintained	**G**

RISK AREAS	AREA CONCLUSION	No of Priority 1 Management Actions	No of Priority 2 Management Actions
Corporate Structure	G	0	1
PCI Scope	G	0	1
PCI Security Controls	A	0	2
Network Security Scans	G	0	1
		0	5

Opinion: Green		
Total: 5	Priority 1 = 0	Priority 2 = 5
Current Status:		
Implemented	2	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	3	

All organisations that take card payments must comply with PCI DSS requirements, which are set by the PCI Security Standards Council to protect cardholder data. OCC take card payments online, over the telephone and face-to-face via Chip & Pin payment devices. Our review has found that significant improvements have been made to the management framework for PCI compliance in recent years, through the introduction of documented standards/procedures and by assigning responsibilities for leading the work in this area.

The overall corporate approach to PCI compliance is set out in the Credit and Debit Card Income Collection Policy and there is an operational PCI compliance programme in place, led by the Income and Banking Systems Manager and supported by IT Services. The Income and Banking Systems Manager has access to specialist advice and guidance on PCI compliance matters. An area for improvement is that there is no formal annual assurance over PCI compliance and addressing this will improve governance by ensuring Senior Management are aware of the status of compliance activities and, specifically, any gaps in control which need to be addressed.

There is no cardholder data held locally on IT systems, which simplifies the PCI compliance regime. A log of all merchant activities is maintained by the Financial Systems and Support team and there is a good understanding of the PCI environment and areas that need to be assessed for PCI compliance, although these would benefit from being formally documented. There is a security policy for Chip & Pin payment devices that requires each merchant site to maintain a local inventory and perform a weekly inspection of the device. Our sample testing identified sites without an inventory and who do not perform a weekly inspection, which could lead to payment devices that have been modified or tampered with not being identified on a timely basis. We also found that the Financial Systems and Support team has not performed a physical annual audit of payment devices as required by the Chip & Pin security policy. Through discussions with the team, it was identified that a physical audit is not an efficient use of limited resources and an alternative approach has been found that will provide the same level of assurance. The Chip & Pin security policy will be updated to reflect this new approach.

A review of telephone payments taken by the Customer Experience Function found they are PCI compliant and the Chip & Pin devices used across the organisation are also PCI approved until 2022. The Capita Pay360 system is used for taking card payments and we tested and confirmed that users have unique accounts and that the password policy complies with PCI requirements. We sample tested five third-party service providers and confirmed their PCI compliance status has been verified.

The training of staff who take card payments is an area that could be improved. From our sample testing at merchant sites, staff confirmed they had received training when Chip & Pin devices were initially installed but a formal record of this is not always maintained and there is no evidence that the training is refreshed. Thus it is not possible to confirm exactly when staff were last trained, which is a risk should this information be required in the event of a data breach.

Approved Scanning Vendor (ASV) scans are not performed as OCC have been advised that they are not required by two sets of PCI consultants based on the scope of the PCI environment. However, the eligibility criteria for SAQ A (Self Assessment Questionnaire), which is used for a number of merchant functions, requires ASV scans and the AoC (Attestation of Compliance), had been incorrectly signed off on the basis that they are performed. Since completion of the audit the errors on the previous SAQs have been notified.

Fleet Management (Compliance) 2021/22

Overall conclusion on the system of internal control being maintained	**A**

Opinion: Amber		
Total: 5	Priority 1 = 0	Priority 2 = 5
Current Status:		
Implemented	0	
Due not yet actioned	0	
Partially complete	0	
Not yet Due	5	

An Oxfordshire County Council review of fleet management carried out in 2019 identified issues arising from the disparate way fleet is currently managed, with vehicle related compliance and assurance, including vehicle safety, taxation, and insurance, as well as driver checks and risk assessments, managed by individual teams within the Council with no central oversight. An audit of Fleet Management was therefore agreed as part of the 2021/22 Internal Audit plan, to test compliance against key controls in this area across directorates, to support the continuing work planned as part of the One Fleet Project.

The audit reviewed compliance in relation to vehicle tax, MOTs, vehicle checks, staff drivers checks, risk assessments and insurance through sample testing of fleet across the Council.

The audit identified a small number of instances of non-compliance with both legal and safety requirements, supporting the need for the new approach. It also highlighted that due to the uncoordinated approach to fleet management, there is no Council-wide assurance or information available on the management and safety of the Council's fleet.

Where compliance issues were identified as part of audit testing, services have been notified and issues corrected. Discussions with the Corporate Director for CDAI confirmed there is the intention for a coordinated approach to fleet management, to facilitate improved oversight of fleet assets and greater consistency in relation to vehicle procurement, management, and disposal.

The audit identified issues with the policies and guidance provided for staff around driving for work, pool cars and hire vehicles, including incomplete and out of date information.

APPENDIX 3

Blue Badge (Disabled Parking) Scheme Enforcement Strategy Oxfordshire County Council

Contents

1. Introduction

1.1 The Blue Badge (Disabled Parking) Scheme provides a national arrangement of parking concessions for people who have an enduring or sustainable disability or condition, including hidden disabilities. It allows Blue Badge holders to park in designated disabled parking bays, as well as in other parking spaces, upon displaying their valid blue badge in the car windscreen.

1.2 There are clear rules around eligibility and usage to ensure the scheme is fair and used appropriately.

1.3 Oxfordshire County Council (OCC) and its partners are responsible for the administration and enforcement of the scheme across the County on behalf of the Department for Transport.

1.4 This Enforcement Strategy aims to ensure genuine blue badge holders are able to make best use of the scheme and to optimise traffic management and parking in hotspot areas. It also provides a framework for dealing with Blue Badge misuse.

2. Types of misuse

2.1 The vast majority of Blue Badge holders use their badges responsibly. However, there are instances of misuse due to the financial and practical benefit associated with using a Blue Badge (parking fees are waived and users can park in disabled bays and double yellow lines).

2.2 The misuse of the Blue Badge scheme undermines its benefits for those who are eligible, impacts upon local traffic management and creates hostility amongst other badge holders and members of the public. It can result in a genuinely disabled person being unable to access designated parking spaces.

2.3 This misuse can take a number of forms including:

- False application for a blue badge
- Use by someone other than the badge holder, either to park in an otherwise restricted area (eg double yellow lines/disabled bays) or to evade parking charges
- Alteration of a genuine Blue Badge
- Creation of a counterfeit Blue Badge
- Use of expired badges
- Use of a badge the holder is no longer entitled to use
- Use of a badge where the holder is deceased
- Use of a badge reported as lost or stolen

This list is not exhaustive.

2.4 It is a criminal offence to misuse a Blue Badge. In the event of someone being found to be in contravention of the Blue Badge scheme, this Strategy seeks to ensure that the Council:

- Clearly messages that misuse of the scheme will not be tolerated
- Provides support to Blue Badge holders to help them to understand their responsibilities as badge holders and reduce misuse
- Enforces the Blue Badge scheme in a fair and consistent manner
- Takes appropriate and proportionate action to disrupt any misuse
- Undertakes criminal proceedings when necessary

3 Roles and Responsibilities

3.1 Currently OCC enforces parking in Oxford City and West Oxfordshire. From the 1st November 2021 OCC takes over responsibility from Thames Valley Police in South Oxfordshire, Vale of White Horse and Cherwell District Council areas. This will ensure equity of parking enforcement across the whole of the County.

3.2 OCC's Parking Team contract with Conduent to enforce the parking schemes in the County. The contract with Conduent stipulates that the Civil Enforcement Officers (CEO's) employed by Conduent will inspect and retain a blue badge when fraud is suspected and provide a written statement to OCC's Counter Fraud Team for further investigation and prosecution. It states that CEO's may also be required to work with the Police, Counter Fraud Officers or any other appointed third-party organization in operations targeting blue badge abuse.

3.3 OCC Officers from the Counter Fraud Team have documented delegated authority to carry out on-street blue badge enforcement exercises and to undertake criminal prosecutions in relation to blue badge misuse.

3.4 Applications for a blue badge are processed by OCC's Customer Service Centre who also act as the first point of contact for members of the public reporting the misuse of a blue badge. This team liaises closely with both OCC's Counter Fraud Team and Conduent.

3.5 All of these teams work closely together in order to implement the Council's Blue Badge Enforcement Strategy.

4 Prevention

4.1 The Council operates an application process which aims to prevent false applications.

4.2 Every successful applicant for a Blue Badge will be issued with the Department for Transport's, 'The Blue Badge scheme: rights and responsibilities in England' leaflet. This will provide the badge holder with the information they need to ensure the badge is used appropriately.

4.3 As part of the application process the applicant agrees to abide by the scheme and not to allow someone else to use their badge.

5 Detection

5.1 Conduent CEO's will inspect vehicles parked using a Blue Badge on the public highway and in Council car parks. Where there is evidence of misuse and the misuse constitutes a contravention of road traffic regulations, the CEO will take the appropriate action as per section 21 of the Chronically Sick & Disabled Persons Act 1970. This may include issuing a Penalty Charge Notice.

5.2 The CEO may also consider seizing the badge and returning it to the issuing authority if they establish reasonable grounds to do so and is practical.

5.3 If the misuse is by someone other than the badge holder, the Council will contact the badge holder to remind them of their responsibility to ensure the badge is not misused and that allowing another person to misuse the badge is a criminal offence. If the misuse continues, the Council will notify the badge holder that further misuse may lead to a refusal to renew the Blue Badge and that the Council may consider criminal proceedings if the misuse continues.

5.4 The Council may receive information on potential Blue Badge misuse from the public, Council employees and other 3rd parties via a dedicated webform on the OCC website. We will consider all allegations made and determine the appropriate action to be taken. Actions may range from reminding the badge holder of their responsibilities to criminal investigation dependant on the individual circumstances of the allegation.

5.5 Where intelligence suggests particular geographical areas of Blue Badge misuse, the Council will consider undertaking operations to target these areas.

5.6 Regular on-street enforcement exercises will be undertaken by the Council's Officers with delegated authority to do so (see Section 6).

5.7 The Council will adopt a proportionate, professional and respectful approach towards any enforcement activity. Badge holders will be provided with an opportunity to explain the circumstances of any potential badge misuse and a reasonable response will be taken. Any safeguarding issues will be referred to the relevant safeguarding teams.

6 Targeted Enforcement Activity

6.1 Regular targeted enforcement exercises will be undertaken by OCC's Counter Fraud Team (approximately 2 days per quarter).

6.2 Counter Fraud Officers will carry out pro-active on street exercises in locations identified by the intelligence received from members of the public and partners such as CEO's, Police etc.

6.3 Officers will inspect Blue Badges they believe to be in use fraudulently and if necessary, seize them. The user of the badge may then be questioned under caution by officers from the Counter Fraud team at the roadside or if deemed more appropriate, invited to attend Council offices for the interview.

6.4 If, however the Counter Fraud Team receives intelligence about misuse by a particular person, the Counter Fraud Team will undertake a targeted one-off enforcement exercise with a view to eradicating the reported abuse / misuse and apply sanctions. This will be used for serious or repeated cases of abuse where a prosecutable offence is occurring. It is possible that such activity would require authorizations such as Directed Surveillance under the Regulation of Investigatory Powers Act 2000 (RIPA) and approval would be sought by the Counter Fraud Team from the Magistrates Court.

7 Investigation

7.1 If the misuse could also constitute other criminal offences (other than road traffic offences), the Council will take the appropriate action to stop the misuse and investigate the offence. The issue of a Penalty Charge Notice for contraventions of road traffic regulations does not prevent the Council from also pursuing criminal offences. Such investigations are not limited to the badge holder, but also include third parties misusing the badge.

7.2 Criminal investigations will be conducted by professionally trained officers from the Counter Fraud Team in accordance with the Criminal Procedures and Investigations Act 1996, Police and Criminal Evidence Act 1984 and any other legislation that may be appropriate to a particular investigation.

7.3 The Council will use the personal data it holds for the prevention and/or detection of crime where it is appropriate and lawful to do so.

8 Redress

8.1 Where evidence of wrongdoing is identified the Council may take one or more of the following courses of action in accordance with the relevant legislation:

- Remind the badge holder of their responsibilities
- Inform the person misusing the badge that they are committing offences and may be prosecuted for future offences
- Retain the badge
- Refuse to renew a Blue Badge
- Cancel a blue badge
- Refuse an application for a Blue Badge
- Offer an individual a formal caution as an alternative to prosecution
- Prosecution

8.2 Where the Council has grounds to believe that the badge holder will permit another person to continue to misuse a badge, the Council will consider refusing to renew the badge once it has expired.

8.3 Where a blue badge holder has been convicted of an offence in relation to the misuse of that badge, the Council will consider withdrawing the badge.

9 Communications and Reporting

9.1 Internal and external communications relating to Blue Badge misuse will be issued for the purpose of preventing misuse or fraud occurring, by educating the public, badge holders and staff on the scheme requirements.

9.2 Internally the outcomes of enforcement exercises will be publicised with the relevant managers and to the relevant elected Councillors, in particular members of the Audit & Governance Committee.

9.3 Outcomes from the on-street enforcement exercises will be publicised externally as appropriate with the support of the Communications Team. This will serve to promote awareness of the enforcement activity which is helpful both as a deterrent to potential or actual fraudsters as well as to reassure residents (in particular genuine blue badge users) that misuse is taken seriously and robustly addressed by Oxfordshire County Council.

9.4 Local media channels such as local newspapers and radio will be used to communicate to residents about enforcement activity. The Communications Team will be consulted on an ongoing basis and in particular at the start of an enforcement activity to ensure that messages are planned in advance, including the use of quotes from elected Councillors where appropriate.

10 Legislation

The Disabled Persons' Parking Badges Act 2013 as amended

The Chronically Sick and Disabled Persons Act 1970 as amended

Road Traffic Regulation Act 1984 as amended

The Fraud Act 2006

Police and Criminal Evidence Act 1984

Criminal Procedures and Investigation Act 1996

Author: Counter Fraud Team, OCC
Last review and publication date: December 2021
Next review date: December 2023
Target audience: Council wide
Subject: Enforcement of the Blue Badge scheme rules