

APPENDIX 2 - EXECUTIVE SUMMARIES OF COMPLETED AUDITS

Summary of Completed Audits since last reported to Audit & Governance Committee May 2025

Social Value Policy 2024/25

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
A: Governance and Reporting	A	0	5
B: Procurement	A	0	2
C: Contract Management	A	0	1
		0	8

Opinion: Amber	
Total: 8	Priority 1 = 0 Priority 2 = 8
Current Status:	
Implemented	8
Due not yet Actioned	0
Partially Complete	0
Not yet Due	0

A: Governance & Reporting

There is a Social Value Policy in place, with a cabinet member and senior officer for social value assigned to lead and govern the policy. The Social Value Policy is accessible on the Council's intranet site.

Internal monitoring and reporting mechanisms exist in the form of a quarterly business report and an annual report on social value that are created in collaboration with Social Value Portal (SVP) (a third-party social enterprise evaluating supplier social value submissions). Day-to-day, the Procurement Policy & Governance Officer, contract managers and others across the Council have access to a live SVP dashboard and can see the status of their contracts from a social value requirements perspective.

A comprehensive learning plan is in place for the procurement team related to the Social Value Policy. New team members must complete this plan within six months. Line managers are responsible for monitoring staff engagement with the plan. However, we noted that the Procurement Policy and Governance Officer does not

receive assurances from line managers on the uptake and completion of the learning plan by their staff.

We noted that contract governance arrangements to oversee the SVP provider could be further enhanced and formalised. For example, standing agendas are not used for contract meetings, and actions are not assigned action owners and due dates in the actions tracker.

The Council were made aware, by SVP, of a recent conflict of interest issue regarding a procurement whereby SVP was responsible for both evaluating the social value tender responses and providing social value consultancy services to one of the bidders. In response, we understand from management that SVP has confirmed that they have put in place additional controls to prevent the issue from arising again and have reported that this is an isolated incident.

B: Procurement

The Social Value Policy outlines the assessment and evaluation criteria for social value commitments, the overall scoring process, and the threshold assessment or exception waiver criteria. The formal contract or terms and conditions with contractors also clearly states the social value commitments made as a part of the winning bidder's response.

We tested a sample of contracts that we understood to contain social value commitments and were being monitored by SVP to validate that all key stages and requirements of the Social Value Policy were followed and could be evidenced. We noted that the listings provided for sample selection were inaccurate as the Social Value Policy was found not to be applicable to some contracts. Other exceptions related to missing documentation to evidence key stages and requirements of the process. A centralised repository to store all Social Value Policy related evidence and documentation does not exist.

C: Contract Management

The Social Value Policy is accessible to all suppliers to give them information and details on how to use the portal as well as the Council's social value expectations. SVP publishes video training materials in their online help centre and clients who have registered accounts can access all the materials available there.

SVP is responsible for monitoring social value commitments made by the Council's suppliers, which includes receiving social value data directly from suppliers, evaluating and validating the data, and making it available within the portal. However, we noted that there is a lack of oversight and understanding of how SVP carries out the evaluation and monitoring process, it has only been verbally communicated. Additionally, although SVP is responsible for ensuring the accuracy of social value data through validation checks as per the engagement letter, management does not have direct oversight of or assurance over these validation processes.

Multiply Controls Assurance 2024/25 (23/24 Grant)

Opinion: N/A	
Total: 3	Priority 1 = 0 Priority 2 = 3
Current Status:	
Implemented	0
Due not yet Actioned	3
Partially Complete	0
Not yet Due	0

The purpose of the Multiply initiative is the delivery of programmes which improve adult numeracy. Oxfordshire County Council received Multiply grant funding for the 2023/24 financial year. The Department for Education (DfE) requires that multiply grant spend for the financial year is audited and reported on and that a copy of the report is sent to the DfE. The grant conditions also require that reporting and sign off from the Chief Executive and Chief Finance Officer is provided confirming that the grant was received and was used for the purposes for which it was received.

Internal Audit reviewed the controls in place in relation expenditure on the Multiply Grant for the 2023/24 financial year, considering receipt of grant income, recording of expenditure, compliance with grant conditions, performance reporting and submission of data returns. Improvements were noted as being required in the following areas:

Processes for the monitoring of delivery - It was reported that there was ongoing discussion and monitoring of progress in delivery of learning against the defined targets, but that much of this was not documented and there had been limited performance reporting produced by the Provider.

Grant Expenditure and Government Returns / Reporting – It was not possible to fully reconcile grant expenditure totals to the Council's finance system. Queries were raised with Finance and with the Service in relation to the differences noted. These were subject to ongoing validation by Finance in conjunction with the Service to ensure any necessary corrections can be made and reported to the DfE. Improvements to reconciliation processes will be embedded for grant spend for 2024/25.

An external QA provider was also commissioned to review the delivery by the Provider. Internal Audit confirmed that the Service obtained some invoice documentation, learner feedback, example learning plans and evidence of learning walks / observations from the Provider, although it is understood that the sample was not directed by the Council (sample provided was determined by the Provider). Controls in this area will be improved for future Provider activity with the Council determining the sample to be evidenced by the Provider for review.

Strategic Contract Management 2024/25

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
A: Governance and Reporting	A	1	2
B: Procurement	A	0	3
C: Contract Management	R	1	5
		2	10

Opinion: Amber	
Total: 12	Priority 1 = 2 Priority 2 = 10
Current Status:	
Implemented	1
Due not yet Actioned	0
Partially Complete	8
Not yet Due	3

Following previous individual contract management audits which identified a mixed picture of the robustness and consistency of contract management, this audit was carried out to review whether strategic contract management is in place both at an organisational level and at an individual contract level for a sample of platinum contracts (all contracts are classified as bronze, silver, gold or platinum, using a consistent scoring tool which uses various factors including contract value, term, and complexity).

The Provision Cycle Handbook was introduced in January 2021 to provide a step-by-step guide on how to undertake commissioning, procurement and contract management activities across the Council. The Provision Cycle Handbook outlines best practice in undertaking provision cycle activities, identifies roles and responsibilities, provides supporting documents and templates, and is intended to promote a consistent and robust approach to the whole provision cycle of which contract management is a part.

In addition to the Provision Cycle Handbook, the Contract Management Framework was updated in September 2021 with the aim of creating a consistent approach to contract management, improving awareness and quality of contract management activity and setting out responsibilities between the Senior Relationship Officer (SRO), the service area and the procurement and contract management hub, in accordance with the four different classifications of contracts (bronze, silver, gold, platinum).

The aims of the 2021 Contract Management Framework have not yet been fully implemented and achieved. The audit has confirmed that there are still inconsistencies in the approach to strategic contract management across the Council. Guidance set out in the Provision Cycle Handbook and Contract Management Framework is not being consistently followed. Contract management plans are not in place for all platinum contracts, although these arrangements are now under review and are being developed to address any gaps that exist. Improvements are required to management information and reporting to provide better strategic oversight of contract management activity and achievement of objectives. Information such as spend analysis is significantly hampered by inaccurate matching of spend information onto contracts.

During the audit it was identified that, as part of the Commercial Transformation Programme, there are multiple projects being scoped to review and improve contract management processes to address weaknesses identified by the Director of Financial and Commercial Services. Management have reported that a number of the issues identified as a result of this audit are already being covered and will be addressed as part of those projects.

Governance

The audit found that there is comprehensive guidance on strategic contract management activity, including that contained within the Provision Cycle Handbook and the Contract Management Framework. These documents are accessible via the Procurement and Contract Management SharePoint site and from the procurement pages on the Council's Intranet.

The Provision Cycle Handbook and the Contract Management Framework both also include guidance on roles and responsibilities for strategic contract management (as well as other aspects of procurement and contract management activity). In addition to this, testing confirmed that job descriptions for relevant roles within the procurement and contract management hub appropriately reflect strategic contract management and related activities.

However, audit testing identified examples where the arrangements in place do not match the guidance set out in the Provision Cycle Handbook or Contract Management Framework. There are inconsistencies in strategic contract management activity across the organisation.

Strategic Contract Management

The Provision Cycle Handbook refers to strategic contract management, in relation to an individual contract, as the process of managing the strategic elements of a contract e.g. resolution of major issues, commercial terms, variations, complaints, overall performance management. This is separate from, and additional to, the processes for *operational* contract management which is the day-to-day management of contracts including tactical issue resolution, administration, payments and so on. Under Strategic Contract Management, the handbook also refers to the development and sign off of a "strategic contract management plan" for each contract.

For the sample of contracts looked at, some strategic contract management activity was found to be in place for most contracts, however from the information provided, inconsistencies in the approach to strategic contract management and how robust and proactive the arrangements are, were noted.

None of the contracts in the sample had a document called a “strategic contract management plan” as referred to in the Provision Cycle Handbook, and in many cases the officers were unaware of the guidance referring to such a document. We found areas of good practice where strategic contract management is in place and appears to be embedded into business-as-usual and working effectively. For example, Public Health has a strategic contract management framework in place for their platinum contracts (three contracts within the audit sample). They do not have specific documents titled “strategic contract management plan” however the activity in place includes the elements that would be included in the plan. For the Adults category, formal contract management plans have recently been implemented for some contracts (including two contracts within the sample) and it is understood that these will be introduced for other contracts within the category. It was also reported by senior management within HESC that the new strategic contract management arrangements that have recently been introduced, together with associated relationships with the strategic providers, are a significant improvement and are working well.

The sample included two platinum contracts for directorate based IT systems, for which we have been unable to confirm what strategic contract management arrangements had been in place during the period reviewed, because the previous senior manager had left without any handover of the contract management arrangements. It is understood effective strategic contract management for these contracts is in the process of being reinstated. This has highlighted a wider weakness in terms of roles and responsibilities for contract management of IT directorate-based applications. With IT applications, as well as the usual contributors i.e. the external provider, the procurement and contract management hub and the service area, there is also the IT service which adds another dimension, and there is more potential for key contract management responsibilities to be missed if everyone is not clear on roles and responsibilities.

Strategic Management Information and Oversight

There is not a consistent reporting mechanism to provide strategic oversight of management information, including achievement or otherwise of strategic objectives and spend analysis. The Contract Management Framework 2021 had identified the requirement to develop a supplier performance dashboard, which would cover reporting on quality, service, cost and risk however this has not yet been implemented. The main aim of the work being undertaken through the Commercial Transformation Programme, is to fully review what is required in relation to contract management across the Council, including roles and responsibilities and processes. Once this part of the programme is completed, management will be in a position to define strategic management information and reporting requirements. Spend analysis is inconsistent and is significantly hampered by inaccurate matching of spend information onto contracts and data quality issues for data recorded in Atamis. Note that the allocation of spend within Atamis is purely for the provision of management information and does not indicate that the actual payments were

inaccurate. However meaningful spend analysis is only possible once the spend data has been significantly corrected. Many of these are known issues and as mentioned above there are projects currently being scoped as part of the Commercial Transformation Programme, to review and improve issues including data & reporting, spend data analysis, and contract management.

The issues identified by the audit include:

- spend is being allocated to the wrong contracts, for example if there are multiple contracts with the same supplier then spend is attributed to the contract with the biggest spend.
- spend analysis is not carried out consistently, it is undertaken on an ad hoc basis or when prompted by a specific need
- there was no evidence provided of spend analysis being reported quarterly to DLTs
- category managers are trying to implement periodical spend analysis however this entails significant effort to first improve the accuracy of the management information
- if the supplier name is not an exact match then spend may be incorrectly categorised as off contract spend
- there is £3.6m of spend attributed to a “test” contract instead of being allocated to the correct contracts.
- fields within the system are not being fully utilised, there are also some where fields are intended to be used but are not used consistently as they have not been made mandatory.
- spend data is usually uploaded into Atamis from SAP every month, however there was recently a gap of 3 months where data was not uploaded promptly
- data housekeeping issues, such as suppliers with more than one supplier name and therefore more than one supplier record
- missing data issues, for example 2 active platinum contracts and 63 active gold contracts have no SRO (Senior Relationship Officer) listed on Atamis, examples where there is no contract manager listed on Atamis including for 4 gold and 10 silver contracts and where contract managers and SROs named no longer appear to be employed by the Council

Supplier Financial Alerts - The Council has a contract with an external provider to provide financial reporting on prospective and ongoing suppliers and to provide automatic updates when there is a relevant change in a company's status, which occurs for various reasons such as a change of director, or a profit warning. If the alert indicates an increased risk to the council in their dealings with the supplier, action may be needed to manage the risk. It was reported that an alerts system is in place and that category managers are receiving alerts, however there is no overall assurance mechanism to confirm that all relevant companies are set up for alerts. It was also identified that there is usually no requirement to repeat due diligence checks on suppliers (such as financial analysis or verifying insurance and other contractual requirements) during the life of a contract, unless the contract is being renewed or extended. This means that those checks might not be carried out for several years.

OCC EYES/LIFT IT Application 2024/25

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
Logical Security	G	0	0
Access Rights	A	0	1
System Administration	A	0	3
Audit Trails	G	0	0
Data Backups	G	0	1
System Support	A	0	3
		0	8

Opinion: Amber	
Total: 8	Priority 1 = 0 Priority 2 = 8
Current Status:	
Implemented	1
Due not yet Actioned	1
Partially Complete	3
Not yet Due	3

The Early Years and Education System (EYES) went live in August 2022 and is the primary system within the CEF Education Service. The Liquidlogic Integrated Finance Technology (LIFT) system went live at the same time for finance and payments within Early Years, Supported Transport and Special Educational Needs. The authentication of users on both systems is well controlled and system backups are performed daily and copies are safeguarded. The main areas for control improvement relate to reviewing user access, system administrator access and performing a post implementation review to confirm the anticipated benefits of EYES have been realised. There is an issue on LIFT relating to errors in payment processes for early years providers which is being managed by finance and ITID (IT, Innovation, Digital and Transformation). Further details on this are given below.

Logical Security:

The systems use Single Sign-On (SSO) for user authentication which confirms a user's identity based on their network credentials. There are a small number of

external users on EYES and the password policy for these accounts is configured in accordance with corporate IT policies. In addition, these users are subject to multi-factor authentication.

Access Rights:

User access within the two systems is defined using 'profiles' and users are allocated a single profile on each system. Each profile has a number of rights associated with it. A review of user access has not been performed since the systems were implemented and hence there is a risk that users with incorrect levels of access are not identified and addressed.

System Administration:

System administration is performed by the ITID Application and System Support team. Members of the team work across all the corporate applications they support to ensure there is no key person dependencies. We reviewed users with system administrator access on EYES and identified some exceptions that should be addressed to ensure privileged access is better controlled. There are a smaller number of users with system administrator access on LIFT and they were confirmed to be valid. The supplier has a number of network accounts which they use for providing support and these accounts are permanently enabled as some of their work is done out-of-hours. The cyber risk associated with leaving accounts enabled should be documented and signed-off at a management level. Sample testing of new starters identified one case where a request for a new account was not appropriately authorised at line management level, which increases the risk of unauthorised access to systems.

Audit Trails:

There is a default audit trail on EYES and LIFT which is not locally configurable. The EYES audit trail is comprehensive and can be searched for key activity, when it was performed, by whom and has details of any changes made. The LIFT audit trail is not as comprehensive and is further restricted in that searches can only be made for a 40-day period at a time. This is a system design limitation and cannot be changed.

Data Backups:

The EYES and LIFT databases are backed up overnight and transaction logs are backed up every two hours. A copy of the backups are held in an air-gapped environment to protect them from ransomware attacks. The systems are designed with a failover capability between the primary and secondary data centres to minimise downtime in the event of an issue or component failure. The failover arrangements reduce reliance on backups for system recovery purposes, although they would be required in the event of a server or database corruption. A recovery test of SQL backups has not been performed to confirm that the database can be recovered within agreed timescales.

System Support:

There is a formal contract for the EYES and LIFT systems, which include support and maintenance. The EYES system was upgraded to the latest version on 10 August 2024. All user support queries are logged with the ITID service desk and any that cannot be resolved by the Applications and System Support team are escalated to the supplier. There are a significant number of open support calls with the supplier

which resulted in the account meetings being replaced by discussions between the previous IT Director and the supplier's Chief Executive. These discussions have now ceased and whilst there has been some improvement in the supplier's performance, it is recommended that the account meetings are resurrected to keep the status of all support calls under review.

A post implementation review of EYES has not been performed to confirm that the stipulated benefits in the original business case have been realised. There are system errors on LIFT relating to the payment of early years providers and the issues are documented and the risk is being managed by Finance and ITID. The system errors are not going to be fixed as LIFT is being phased out by the supplier and will be replaced with ContrOCC for early years payments from April 2025. The implementation of ContrOCC should be fully tested and only signed off once it is confirmed there are no processing errors.

Cyber Security Review 2024/2025

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
User Education and Awareness	G	0	0
Malware Scanning	G	0	1
Supply Chain	A	0	3
Incident Response Plan	G	0	0
		0	4

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

Cyber security continues to remain one of the biggest risks faced by organisations, given the almost endless reports of security incidents, data breaches, ransomware, phishing and other cyber-attacks. All organisations reliant on technology systems are vulnerable to cyber-attacks and must operate strong security controls to minimise the risk of any attack being successful. The review found there are good controls in

place over user education and awareness, malware scanning and cyber incident response planning. In recent years there has been a significant increase in the number of cyber-attacks resulting from vulnerabilities within the supply chain and this is an area where controls need to be strengthened to ensure risks are being effectively managed.

User Education and Awareness:

All users are required to undertake mandatory training on cyber security and in April 2024 it was confirmed that all current users had completed their training. This is an excellent achievement. The cyber training is being refreshed for 2024-25 and the new training will be bespoke for some service teams and more interactive for everyone else. Phishing simulation exercises are performed and users who click on the link within the test email have to undergo additional phishing training. Key messages on cyber, including details of any specific threats, are communicated via Yammer and directly on email when it is deemed more urgent.

Malware Scanning:

A defence in depth approach is adopted to scanning for viruses and other malware threats. The antivirus software installed on computer endpoints was reviewed and found to be suitably configured, maintained and monitored. Coverage of antivirus software should be extended to include corporate Android devices as they are susceptible to malware threats. Internet downloads are scanned for malware by a separate tool which also blocks access to malicious websites and capital funding has recently been secured for a new Endpoint Detection & Response (EDR) solution which will further strengthen security against malware and other cyber threats. ITID subscribe to the National Cyber Security Centre (NCSC) Mail Check and Web Check services.

Supply Chain:

A set of ICT technical requirements are documented for new technology procurements and include areas of cyber security. Beyond this there is little evidence of any management of cyber risk in the supply chain. A review of existing suppliers has not been performed to identify those that pose the greatest cyber risk, cyber security is not included within contract management arrangements and contractually there is no obligation on suppliers to maintain any confirmed cyber security certifications, such as ISO27001 and Cyber Essentials, during the life of the contract.

Incident Response Plan:

The documented Cyber Incident Response Plan has been maintained and was tested in May 2024 as part of a council-wide business continuity exercise. The exercise was based on a cyber incident affecting the supply chain. The ITID actions from the exercise have been completed.

Identity and Access Management Review 2024/25

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
Governance and Oversight	A	0	2
Accounting Provision	A	0	5
Account Deprovisioning	A	0	2
Movers	A	0	1
User Authentication	G	0	0
Third-Party Accounts	G	0	1
		0	11

Opinion: Amber	
Total: 11	Priority 1 = 0 Priority 2 = 11
Current Status:	
Implemented	0
Due not yet Actioned	1
Partially Complete	0
Not yet Due	10

Identity and Access Management (IAM) is a framework of processes, policies and technologies that are implemented to control user access to digital systems, data and resources. The audit has found that the identity of users is appropriately verified at a network level but the controls around the management of user accounts can be improved. This includes the provisioning and deprovisioning of accounts as well as access for users who change roles. Third-party accounts are generally well managed, although we have identified that agreed procedures are not always followed.

Governance & Oversight:

The area of IAM is covered within a number of documented IT policies, which are all current and valid. A review of the policies found they cover the provisioning and deprovisioning of user accounts and third-party access but do not have any details on authorisation requirements for new user accounts or managing access for users who move roles within the Council. The procedures for managing starters, leavers and movers is not documented to define operational processes and also specific

roles and responsibilities. There is a dedicated systems administration team within ITID who lead on the day-to-day management of user accounts.

Account Provisioning:

New user accounts are requested using an online starter form that is available on the Intranet. Any existing user can request a new account and they self-certify that they are authorising the person's access. No further authorisation is sought, which increases the risk of accounts being created for unauthorised access. The starter form requires the name of an existing user whose permissions are copied, which is bad practice as it assumes that the copied account has the correct level of access.

New accounts for permanent employees require the National Insurance (NI) number to be supplied so that their network account can be linked to their IBC record. A copy of the NI number is retained within the user's network account profile. The use of the NI number should be reviewed by the Information Governance team to confirm processing is in accordance with Data Protection requirements.

New users are added to security groups depending on which service area/team they work in but membership of groups is not subject to any formal review. Scripts have been developed to automate many of the tasks relating to user accounts and formal documented procedures are required to confirm how changes to scripts should be managed and tested.

Account Deprovisioning:

There is a process for managers to report leavers to ITID so that their user accounts can be disabled. We tested a sample of recent leaver reports and confirmed that the system is working effectively and that user accounts have been deleted. The current system for leavers is reliant on ITID being notified by managers as they do not receive any leaver reports from HR or review accounts to identify any that have not been accessed for a defined period of time. There is therefore a risk that not all leaver accounts are deleted on a timely basis. All accounts for temporary users, such as contractors, are set with an expiry date.

Movers:

For users who change roles, a movers form is used to request their security group permissions to be updated. The current procedure has the same risks as reported above for new starters as mover requests are not authorised and the new access is copied from an existing user.

Security groups classified as "restricted" are not automatically added as part of the mover process but we found that not all groups are classified, hence any which are not but hold sensitive data could inadvertently be given to the user. Some security groups are managed locally by service areas and it is their responsibility to remove movers from these groups but this does not always happen, which leaves a risk that movers retain access to network files they do not need for their new role.

User Authentication:

The requirements for user authentication are defined within corporate IT policies and there is a robust password policy for authenticating the identity of network users. Previous audits have confirmed that multi-factor authentication is used for remote access. For new accounts, a strong password is generated which has to be changed at first login by the user. There is audit logging of user activity, which includes logon

and logoff times, should this information be required to investigate security incidents or suspicious activity.

Third-Party Accounts:

There are procedures in place for managing third-party accounts, which includes a process for requesting them to be enabled and then only for a specified period of time. We sample tested five supplier accounts that were enabled at the time of the audit and found two which had no expiry date and where the service desk reference is from the old system so no details are available. One other open account was not linked to any service desk ticket. This presents a risk that supplier accounts are left open for longer than required and could be compromised in a cyber-attack.

Direct Payments 2024/25

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
A: Governance, Policies & Procedures	A	0	13
B: Direct Payments Operational Processes	A	0	5
C: Direct Payment Usage	A	0	13
D: Payment Accuracy	G	0	4
		0	35

Opinion: Amber	
Total: 35	Priority 1 = 0 Priority 2 = 35
Current Status:	
Implemented	1
Due not yet Actioned	0
Partially Complete	0
Not yet Due	34

Children’s direct payments are made on behalf of Children’s Social Care, Education and Health. These arrangements are either via a managed account or are self-managed by a representative of the child. The need for a children’s direct payment is determined by Children’s Social Care, Education or Health, with advice and guidance on the set up of the direct payment provided by the Direct Payment Advice Team (DP Advice Team), with the exception of Education. Direct payment arrangements are set up, paid and overseen by different parts of the Payments & System Data Team which sits with Adults Social Services.

The key areas for improvement identified from audit testing relate to differences in approach to Education direct payments, in ensuring that all relevant children's direct payments are identified for audit by the Direct Payment Audit Team (DP Audit Team), that there is clarity over the process, roles and responsibilities for responding to queries resulting from direct payment audits (DP audits), in relation to the oversight of managed accounts, and in ensuring that there is an appropriate approach in place for the monitoring and clawback of children's direct payment account balance surpluses. There is also a need to review the need for and develop management information on children's direct payments for service areas.

Governance, Policies & Procedures – Within Children's there is a mix of self managed and managed direct payments. Online direct payments, which provide greater oversight to the Council on spend and balances, are not used. It is noted that there is no overarching strategy or approach within Children's over the use of direct payments (for example to promote the use of managed accounts where possible) and no guidance on children's direct payments on the Council's website.

There are defined processes in place within Education and Children's Social Care in relation to the set up and ongoing consideration of children's direct payments, however the approach, particularly within Education, has evolved and is not consistent with direct payment processes in other parts of Children's or Adults. For example, a different form of direct payment agreement is used, the DP Advice Team (whose role is to ensure that direct payments are set up consistently and correctly and provide support and guidance to direct payment recipients / their representatives), until very recently, have not had any involvement in the set up of Education direct payments. These payments are set up for a year at a time rather than being ongoing.

It is positive to note that discussions are already taking place between Education, the DP Advice Team and the Payments and System Data Team to determine how education direct payment processes can be more aligned and how the different teams can work together more effectively. There is a need to clarify roles and responsibilities in relation to direct payment audit activity for Education staff including how DP Audit Team queries should be reviewed and responded to and how the escalation process should work.

In relation to Children's Social Care, whilst they have clearly established processes for setting up and administering direct payments, team level staff guidance is not in place and there are some areas where roles and responsibilities require clarification (for example in relation to the direct payment review process).

The Payments and System Data Team process and pay children's direct payments on behalf of Health. However, as highlighted in the 2023/24 Health Funded Payments audit, there is no signed Memorandum of Understanding or Scheme of Delegation in place which clarifies who the team should accept instructions from or how these instructions should be authorised. Management action to address this was agreed as a result of the separate audit report, but as yet, this has not been implemented.

There is no reporting or management information being produced on children's direct payments for Education or Children's Social Care operational teams or for senior management within Children's in terms of direct payments processed, being made, being audited etc. It is noted that since the previous audit of Adults Direct Payments

in 2022/23 reporting dashboards have been developed to monitor and report on DP Audit team activity.

Direct Payments Operational Processes – Some delays were noted between approval of funding for a direct payment and the submission of the request to the Payments and System Data Team to set up the arrangement. Within Education, it was acknowledged that there are different factors which have caused delays, these include team capacity but also delays in being able to obtain signed agreement from parents / carers as a result of dissatisfaction with the level of support agreed. Improvements to the process for the arrangement of new direct payments within Education including the input of the DP Advice Team should assist in minimising some of these delays going forward.

In terms of Children's Social Care direct payments, there were some cases where delays were noted between panel approval and the submission of the request for the direct payment to be set up, however it was reported that these delays were mainly in relation to completion and sign off of direct payment agreements which must be completed prior to payments commencing and involve working with DP recipient's representatives.

From review of the way in which direct payment operational processes are working within Education, it was noted that the current process (designed prior to the implementation of the EHM system) for referral from the service to the Payments and System Data Team is electronic form / email based. This requires review to determine whether there would be benefit or efficiencies in developing an automated workflow process (which is in place for Children's Social Care and Adults direct payments) to approve new arrangements and communicate requests through to the Payments and System Data Team. There is also a need to review and align the agreement signed by the representative of the direct payment recipient with other service areas and ensure that it appropriately covers aspects including document retention periods and DP Audit Team activity.

Whilst both the service areas and the Payments and System Data Team (DP Audit Team) have processes which include review of the direct payment arrangement, these processes are not co-ordinated and do not inform each other in a systematic way. There is also a lack of clarity / consistency in what coverage of direct payment use is expected as part of the service based review. Although issues or queries raised as a result of a DP audit would be flagged with the relevant contact in the service (although there has been a lack of clarity over who should be contacted within Education and over roles and responsibilities in this area), there isn't any routine information provided on when cases were last audited unless this is specifically requested. Within service areas, although the use of a direct payment should be considered as part of the review process to some extent, there is no clear guidance which sets out what should be considered and what should be flagged with the DP Audit Team.

Direct Payment Usage – The methodology and approach used by the DP Audit Team to determine the frequency of audit of direct payment accounts has recently been reviewed, with a revised approach implemented for adults direct payments. Children's are to be consulted on the proposed changes. There is also a need to review and clarify the escalation process where issues are noted with DP audits of children's direct payments. Whilst queries are referred back to a contact within the

service area in the first instance, there is no agreed escalation process following on from this for Children's.

The audit noted 5 education direct payments which had not been audited as they had not been set up correctly in the DP audit workspace. For other direct payments, the workspace is set up on LAS by the DP Advice Team, however at the time of testing, they were not involved in the set up of education direct payments (instead the workspace should have been set up by the Systems team). There is also no control in place to enable reconciliation of direct payments being made to those being audited and provide assurance that the cases subject to DP Audit are complete.

It is noted that accounts managed by one of the managed account providers are not subject to audit by the DP Audit team. There were specific issues and concerns with this managed account provider highlighted as a result of previous audits of direct payments in Adults, but it has been noted that the process has not changed.

Testing noted that there is a lack of appropriate process in place to monitor, query and, where appropriate, clawback children's direct payment account surplus balances. Self-managed and managed account surpluses are monitored and queried through the DP Audit process; however weaknesses have been noted in the completeness of the DP Audit programme which means that some accounts with surpluses have been and could continue to be missed. The process in relation to one of the managed accounts providers requires review as although there is 6 monthly reporting on surplus balances, it was reported that a previous agreement with Children's means that children's direct payment accounts highlighted on the report are not followed up and surplus balances are not returned. The process for the clawback of surplus balances, particularly for managed accounts was an area for improvement highlighted as a result of 2022/23 Adults Direct Payments audit. The management actions agreed have been noted as not having been effectively implemented.

During previous audits of direct payments, a lack of systematic quality assurance processes in relation to the work of the DP Audit Team was noted. Although management action to introduce quality assurance processes had been reported as fully implemented, this could not be evidenced. Testing noted several areas where there were either errors or delays in the DP Audit process which had not been picked up prior to the audit. Although these examples were not material, the lack of systematic management oversight and quality assurance means that it would be difficult to identify and promptly address any significant issues that did arise.

Payment Accuracy – Testing on a sample of children's direct payments confirmed that payments are being made accurately and promptly once instructions are received by the Payments and System Data Team.

Some issues were noted in relation to the accuracy of cost centre coding for some direct payments as a result of an erroneous temporary change to budget derivation rules on ContrOCC. Management actions have been agreed which will identify and enable correction of incorrect coding and review and update system permissions to prevent this type of change reoccurring in future.

During scoping, the team reported that they were in the process of changing the frequency of invoicing to Buckinghamshire, Oxfordshire, and West Berkshire Integrated Care Board (BOB ICB) to recover direct payments made on their behalf,

moving from annual to quarterly invoicing. It is understood that invoices for 2023/24 and 2024/25 to date are in the process of being agreed with BOB ICB.

Follow Up – As part of this audit, we followed up on the implementation of 7 management actions agreed as part of the 2022/23 Direct Payments audit which related to processes covering both adults and children’s direct payments. 3 were confirmed to have been implemented effectively. 4 could not be confirmed to have been implemented effectively, these actions relate to the finalisation and circulation of DP Audit Team Guidance, the confirmation and implementation of a quality assurance process for DP Audit Team activity, agreement and implementation of a process for the audit of managed accounts and the review of segregation of duties in the DP Audit and surplus recovery process. Revised or restated management actions have been included in the detailed findings section of the report below.

Highways Contract 2024/25

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
A: Existing Contract Closure and Transition to New Contract	G	0	1
B: Re-establishing Contract Governance (New Contract)	A	0	1
		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

The audit was performed during the transition period from the old to new contract. As of early December 2024, the new Highways contract is in the final stages of clarification with Milestone and is due to be agreed and signed off by both parties before the end of December. As such, our discussions, testing and review of documentation focused on current and future transition programme activities, some of which have not started yet but are scheduled to be carried out at a later date. Our conclusions do not cover the implementation or design of processes which are still being developed.

Overall, there is a good system of internal control in place and the majority of risks across the areas of scope reviewed are being appropriately mitigated. The approach developed to transition from the old to new contract has been designed in a robust manner. We noted improvements could be made in relation to the implementation of a system/digital platform to more effectively manage compensation events, reducing the risk of manual error and the review and re-prioritisation of existing timelines for training activities to better facilitate the smooth execution of the new NEC4 contract from the 1 April 2025.

A: Existing Contract Closure and Transition to New Contract

Following the tender exercise and the Council's decision to award the new contract to Milestone (the incumbent), a Demobilisation and Mobilisation programme was formally approved. The various workstreams within the two programmes, which are aligned to the workstreams in Milestone's tender submission, contain numerous tasks and activities that once completed, will enable the Council to transition from current ways of working under a NEC3 contract (New Engineering Contract), to new ways of working under a NEC4 contract. The transition from NEC3 to NEC4 involves changes in governance and management practices. The main differences relate to ensuring more specific governance structures for different project types, early contractor involvement to improve project outcomes, encouraging collaboration and proactive problem-solving, a more structured approach to risk management with enhanced risk register processes, making governance more robust, a new tier of dispute resolution, including the option for Senior Representatives and Dispute Avoidance Boards, which aids in resolving disputes more effectively without escalating them, and more flexible payment options.

A governance structure has been established to monitor the progress of the two programmes with the two key governance groups (Demobilisation and Mobilisation Steering Groups) meeting on a bi-weekly basis. The governance structure also includes reporting from those two key groups up to the Council's Highways Operations Board for escalation and decision-making purposes. Formal terms of references and set agendas are in place for both steering groups and highlight reports providing a RAG grading on the status of each workstream are produced for discussion during the meetings. Each workstream has a lead from the Council and a lead from Milestone. Key elements such as stakeholder engagement, risk management, communication channels and training form part of both of the programmes and are at various stages in terms of their formalisation. For example, specific risk registers are in place for Demobilisation and Mobilisation, which are also reviewed and discussed during the bi-weekly meetings.

Whilst we noted the Mobilisation programme has a workstream dedicated to training, training materials are still in development with planned timescales for rollout running until the end of March, just before contract go live on 1 April 2025. This timescale does not leave any room for delays or slippage. Given the scale of change from operating under a NEC3 to NEC4 contract is extensive, there is a risk that without bringing forward the development and roll-out of formal training over the next 3-4 months, the transition process may not be as effective and smooth as planned.

Overall, transition plans are robust and clearly outline and define the Council's approach to contract closure of the existing contract and the formal acceptance of project deliverables, objectives and commitments under the new contract.

B: Re-establishing Contract Governance (New Contract)

Milestone's tender submission documents outline their proposals in regard to governance, decision-making, problem resolution, escalations, performance management and change management. The proposals are based on the requirements and specification outlined in the Council's contract scope and specification document and are now being reviewed and formalised as part of the formal Mobilisation Plan.

The contract scope document details the respective roles, responsibilities and accountabilities of both the Council and Milestone in relation to maintaining the network, prioritisation and programming, policy and strategy, customer and stakeholder engagement, asset management, design and network management.

The contract scope document also provides clarity on the list of qualifying compensation events under the new NEC4 contract. A compensation event is defined as an event that, if it occurs, entitles the contractor to claim additional time and/or money. They are specific occurrences that are identified in the contract as giving rise to a potential change in scope, timing or cost of the works, and thus necessitating an adjustment to the contract's terms. Whilst the scope of compensation events is clear, there isn't currently a system in place to manage compensation events under NEC4. Current ways of working are manual in nature and therefore prone to human error and risk. A system / digital platform to manage compensation events would provide centralisation, automation, less manual intervention, more effective monitoring and robust document management.

Income Collection Street Works and Parking 2024/25

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
A: Governance, Roles and Responsibilities	A	0	3
B: Fees and Charges	A	0	2
C: Income Collection	A	0	5
D: Surplus Spending	A	0	1
		0	11

Opinion: Amber	
Total: 11	Priority 1 = 0 Priority 2 = 11
Current Status:	
Implemented	0
Due not yet Actioned	0
Partially Complete	0
Not yet Due	11

Overall, the audit found that there is generally a good system of internal control in place in relation to parking and enforcement related income collection processes and for surplus spending from the parking account. We have found areas for improvement in relation to street works income collection processes and surplus spending controls. We also noted some areas for improvement to enhance overall governance and monitoring controls such as maintaining up to date procedure notes and maintaining records of key activities and decisions taken.

A: Governance, Roles and Responsibilities

Cabinet is engaged in decision-making and approvals relating to the street works and parking service. They are also responsible for reviewing and approving discretionary fees and charges (i.e. those determined by the Council) on an annual basis and any in-year changes (if applicable). On an annual basis a Parking Services report is produced providing an overview of the service including key performance outcomes and income collection parking statistics for the different parking incomes streams. Monthly meetings are held between the Head of Network Management and the Director of Environment and Highways, and regular programmed meetings also take place with Finance Business Partners. At present, no notes are formally kept capturing key points discussed, decisions made and/or actions agreed at these meetings, picking up on the formal forecasts made and agreement as to what is reported within the monthly Business Management and Monitoring Report (BMMR).

There is an overarching Parking Policy, outlining key objectives and aims of the service but the document has not been updated since September 2014 to reflect current objectives, priorities, risks, roles and responsibilities. It is reported that this work is currently in progress.

The Council's Financial Regulations outline general requirements in relation to income collection however this is pitched at too high a level to be used as the only set of governing procedures for street works and parking income collection. We understand that process maps are in development but not yet completed and approved. Given the wide variation in income collection processes that are required across street works, parking and enforcement, a set of detailed procedures would provide a more robust control framework. It is reported that this work is in progress.

B: Fees and Charges

A fees and charges matrix is produced that contains all fees and charges whether discretionary (i.e. determined by the Council) or statutory (i.e. set by external bodies such as the Department for Transport). Once approved, this is accessible on the Council's website. Fees and charges for street works permits and street works coordination are aligned to statutory guidance (i.e. the maximum levels set by the Department for Transport). On-street parking fees and residential permit fees are set

by the Council. Parking pay and display income is collected either directly at the pay and display machine or via third party applications such as RingGo, PayByPhone and Just Park. Parking enforcement related income is collected on behalf of the Council by a third-party contractor.

Council approved fees and charges are loaded into pay and display machines and other third-party applications / systems used for parking and enforcement income collection. Street works related fees and charges are loaded into the Street Manager tool. Regular checks to confirm the correct fees and charges have been loaded across all platforms/systems used is carried out (the Council has access to the back office of third-party systems to check and verify the accuracy of fees and charges).

For a sample of street works and parking income transactions, we checked that the fees and charges applied agreed to the fees and charges matrix approved by Council. For the majority of transactions sampled, fees and charges agreed to the fees and charges matrix. Where there were discrepancies or it was not clear, explanations were provided, however the supporting evidence to validate the explanations was not available in some cases.

C: Income Collection

We assessed the controls in place for each of the in-scope income streams. We found that for the majority of income streams (namely Temporary Traffic Regulations Order (TTRO) income, Parking income (pay and display, third party apps and permits) and Enforcement income) there are appropriate processes in place relating to the collection of income and from the samples tested, no exceptions were noted.

However, we have noted areas for improvement in relation to Street works (Permit fee and Co-ordination income):

Permit fee income relates to permits applied for by utility companies for street works. Co-ordination income relates to Section 74 overruns charges, inspection fees and other penalties. Street works activity is logged in Street Manager (a government system, not the Council's). For permits, S74 overruns and inspection fees, invoices are raised based on a download of data extracted from Street Manager via a software called HIAMS. Other penalties are not invoiced. Instead, utility companies are notified of the penalty via Street Manager, and they are responsible for making payment directly to the Council, in accordance with DfT guidance. We noted the following findings from our testing:

- Regular reconciliations between the data held in Street Manager and what is invoiced and receipted through SAP to confirm the completeness of income are not carried out.
- There were examples where queries were raised with the service during audit testing and whilst explanations were provided, these could not be evidenced with appropriate supporting documentation.
- In our testing of co-ordination income, we identified a 'sweep' journal entry that was made up of three payments. One of these appears to be incorrectly coded as it relates to permit fee income for one utility company for the months of January – October 2023. From our review of the transaction listings provided, we noted that the permit fee income is recorded in two cost centres and therefore appears to be double counted. We enquired with management, however the reason for this error has not yet been understood and requires investigation with the Finance Help Desk.

In relation to budget monitoring, budget versus actuals analysis is carried out monthly, across all of the above income streams, by the Head of Network Management. Where significant variances, trends and any unusual transactions/movements are identified these are investigated further. An example of how this control has operated successfully in recent months was shared during the audit whereby parking enforcement income for contraventions caught on camera was coming in lower than budget in the first three months of the FY23/24 financial year. This was raised with the enforcement contractor, and it was discovered that a technical error led to Penalty Charge Notices (PCNs) not being issued. This has resulted in an approximate loss of income of £250k for which the enforcement contractor is contractually responsible to reimburse the Council. The legal process to recover this income is ongoing.

D: Surplus Spending

Section 55 of the Traffic Management Act 2004 outlines the requirements in relation to spending surplus money from the Council's parking account. The Council has a formal process in place to ensure regulatory requirements are met. The process includes the preparation of a business case for the spending and subsequent review and approvals sought. One proposal was submitted by the Head of Network Management during the year. We obtained the supporting documentation and confirmed that it received appropriate authorisation from the Director of Environment and Highways as per the Council's delegated authority.

For street works surpluses, DfT guidance (Permit schemes: statutory guidance for highways authorities - July 2022) outlines the requirements for spending surplus money relating to permit fee income. Regulation 32 stipulates that fee income must be applied 'towards the costs of operating the permit scheme which are prescribed costs'. If there is a surplus in a given year, the money should be applied towards the costs of the scheme in the next year and the fee levels adjusted accordingly. A sustained surplus where the income was regularly exceeding the prescribed costs would indicate that the fee levels should be adjusted. For other street works income streams, surplus funds can be used across the service in any way deemed most appropriate. Unlike parking surpluses, formal review and approval controls could be strengthened to govern the spending of street works surpluses.