Appendix A

7

Internal Audit and Counter Fraud

Quarter 2 Progress Report 2020/21

CONTENTS

1. Summary of Completed Audits

School Safeguarding Arrangements Follow-Up (2019-20)

7

1.1 Section 175 of the Education Act 2002, states that: 'the local education authority shall make arrangements for ensuring that the functions conferred on them in their capacity as a local education authority are exercised with a view to safeguarding and promoting the welfare of children'. The Education Safeguarding Team (EST) fulfils this responsibility by engaging with all the education providers to improve their processes and help them to deliver.

1.2 An audit of the EST in 2018-19 found poor systems and controls in place, which led us to give an opinion of Minimal Assurance. This follow-up audit was included in the agreed annual audit plan for 2019/20 and was undertaken to provide assurance that new systems implemented by management had improved the control environment.

1.3 The scope of the audit sought to ensure that adequate controls were in place to provide assurance that:

- A suitable system had been implemented to obtain assurance over education providers' safeguarding arrangements;
- Effective frameworks had been established to provide support to education providers when safeguarding issues arose, to ensure compliance with relevant legislation; and
- Current and emerging risks in relation to education providers' safeguarding arrangements were adequately considered within the Schools and Learning risk register.

1.4 We identified that controls had greatly improved within the processes and systems used by the EST. Examples of where improvement had occurred included:

- The launch and use of a new online self-assessment portal called 'Enable', to allow education providers to complete and submit returns on their safeguarding arrangements. At the date of our audit 86% of education providers had signed up to using the portal, a significant improvement on previous years;
- Appropriate training and support had been provided to members of the EST and education providers following the launch of the online portal; and
- Progress made in paving the way for sharing information and intelligence to produce a 'schools causing concern register'. This is expected to assist in co-ordinating services across the directorate and with Schools Alliance for Excellence (SAfE) to help the service to develop further an effective risk-based approach in identifying schools requiring additional support and challenge.

1.5 Whilst the EST has taken numerous steps to make improvements to date, the audit did note that further work remains to determine how the safeguarding arrangements for children placed in out of county settings should be assessed. The team also need to take necessary measures to require the remaining 14% of education providers to sign up to the online portal. We agreed actions with management in both respects.

7

1.6 Given the improvement in overall control, we gave an uprated opinion of Reasonable Assurance.

Use of Consultants – Policy for the Use of Interim Workers (2019-20)

1.7 The council's workforce includes individuals engaged on a temporary basis to ensure we have the right people, with the right skills, in place to meet business needs. The use of temporary workers can offer numerous benefits, including continued service delivery through cover for vacancies, extra capacity to deliver projects or additional work, and access to specialist expertise not otherwise available.

1.8 In support of the council's transformation journey, in the 18 months preceding the COVID-19 pandemic the use of external interim workers increased significantly. A new "Policy on the Use of Interim Workers" was developed by HR&OD in autumn 2019, aimed at ensuring the application of robust and consistent engagement processes, maximising value for money, and ensuring compliance with HMRC and other relevant legislation.

1.9 The purpose of our audit was to provide assurance that controls were in place to meet the following objectives:

- The policy was robust and considered all aspects of the use of consultants or interim workers;
- The use of consultants or interim workers was supported by appropriate guidance and policies; and
- All relevant policies and guidance have been effectively communicated to managers.

1.10 We concluded that all aspects of the engagement and management of interim workers had been combined within a robust single policy. Aspects of the policy were slightly amended in response to our initial findings as the audit progressed. The policy was also presented to the Council Leadership Team as a draft and amended in response to their feedback.

1.11 Whilst HR&OD had consulted with Procurement prior to finalising the policy, discussions with IT&D were more limited and we identified the potential for the policy, as originally audited, to unintentionally cause a breach of the IT Security Policy relating to the use of personal IT equipment. We acknowledge, however, that this section of the policy has now been re-worded, and we also recognise that certain transformation programmes and the 'Agile' agenda will likely lead to further changes to these IT policies.

7

1.12 The effectiveness of the policy was potentially hampered by a lack of awareness of its existence by managers, due largely to communication of the new policy being limited to a group email to senior managers and the policy being absent on S-net. There is, however, guidance on legislation available on S-net, which was enough to support managers in meeting IR35 requirements.

1.13 Overall, we were able to give an opinion of Reasonable Assurance following our audit, with actions agreed with management to address the issues identified.

Cloud Computing (2019/20)

1.14 Cloud computing is the technological capability to use IT infrastructures and services that are not installed on a local computer or server. Using the internet, connections are made to external computers or servers that provide appropriate resources. Unmanaged, cloud computing creates significant risks to the security of the council's systems and data.

1.15 From a sample of applications and systems retained in the cloud, we reviewed the controls in place to manage the security, access, recovery and deletion of the data. The governance arrangements for managing the use of cloud-based systems were also reviewed.

1.16 Our sample of cloud-based systems reviewed was:

- BookWhen (in Children, Families, Lifelong Learning & Culture);
- Adobe Creative Cloud (in Surrey Fire & Rescue);
- Career Vision/Serelec (in Children, Families, Lifelong Learning & Culture); and
- Infogram (in Corporate Resources).

1.17 We were able to provide Reasonable Assurance over the controls operating within the area under review because IT&D have in place comprehensive and robust risk assessment processes that take place prior to the implementation of any cloud-based system. Information provided on

the council intranet site specifically stresses the importance of contacting IT&D prior to procuring cloud-based software.

1.18 Good practice was demonstrated in our sample in respect of services updating their Privacy Notices in line with the implementation of the cloud-based systems, an adherence to Data Protection legislation, including the General Data Protection Legislation, as part of their terms & conditions, and the existence of suitable arrangements should system outage occur.

7

1.19 However, one area of concern identified that officers can procure cloud-based systems without going through IT&D or Procurement. This is due to a lack of technical controls in place to prevent systems being procured using a purchasing card. For each of the systems selected in our review, IT&D were unaware of its use within the specific service. As such, these systems present a risk to the security of the council's data as they had not been subject to IT&D's usual governance procedures. We also identified some weaknesses in specific systems that once addressed through the agreed actions, will improve the overall control environment.

Patch Management (2019/20)

1.20 With ever increasing reliance on computer systems, an effective patch management process is crucial to ensure that critical security weaknesses are promptly closed, and systems remain available and up to date. However, patch management processes need to ensure systems can continue to work effectively with other hardware and software following the application of a patch.

1.21 Our audit was undertaken with a focus on patching in relation to desktop and laptop devices via Microsoft System Centre Configuration Manager (SCCM), and a sample of critical systems hosted on-premises (namely SAP and ContrOCC). Infrastructure patching arrangements (including servers and switches) were not included within the scope of the audit as these had been previously reviewed within our Cyber Security audit.

1.22 We were able to provide Reasonable Assurance over the controls operating within the area under review because:

- Good practice was demonstrated in relation to patching, as patches were identified and deployed in a timely manner to relevant council devices;
- Patches and updates were applied with consideration to balancing the benefits of patching against the risk of doing so, and the need for user convenience; and

- Vulnerability scanning takes place, identifying instances where patches are required, as opposed to where software has reached the end of operational life.

1.23 However, some weaknesses in the control environment were identified, including:

- A lack of oversight of patching at a council-wide level, with reports on the council's patching status not being routinely run by management. This could result in applications not being appropriately updated, leaving them vulnerable to security incidents;
- The council's Patch Management Policy was out of date, containing obsolete information and missing key metrics, such as target times for patches to be applied;
- Patches applied to desktop and laptop devices were not tested prior to deployment, meaning systems may become unstable or inaccessible should the patch conflict with other software or other hardware; and
- End-of-life software, for which patches are no longer available, was not routinely documented or monitored, so the council could continue to use unlicensed or insecure software.

1.24 Actions were agreed in relation to two medium and three low risk findings to address these the above issues.

Mobile Device Management (2019/20)

1.25 Mobile devices such as smartphones and tablet computers have the capability to store large amounts of data and so can present a high risk of data leakage and loss. Such devices are often valuable and are therefore also vulnerable to theft and/or misuse.

1.26 Mobile device management (MDM) involves monitoring, managing and securing mobile devices to ensure that the council's information assets are not exposed. MDM is usually implemented through third-party software. The council's MDM solution is provided by VMware AirWatch and covered (at the time of our audit) 4,476 smartphones and 593 tablet computers.

1.27 Our audit considered the council's approach to managing the risks associated with the security and control of the data contained on smartphones and tablets. It did not review the controls in place for managing the contractual payments for calls and data, or the procurement of the devices, nor did it cover the management of laptop devices as these are managed through different processes and procedures.

1.28 Overall, we gave an opinion of Reasonable Assurance over the controls associated with the management of mobile devices because:

- Security policies (including rules for appropriate physical and logical handling of mobile devices by the end-user) had been developed;
- The MDM system enforces policy-based controls to help manage, monitor, and secure mobile device that access and/or store corporate data;
- The system can lock or wipe managed devices remotely in the event of loss or theft;
- Security settings configured on the MDM system were consistent with the council's IT security policies (except for password format rules);
- Devices are automatically placed in a non-compliant status (where functionality is suspended or restricted) if the device fails to apply one or more security policy settings, or the user has not complied with the policies;
- The ability to install third party applications on managed devices had been restricted and users can only install applications that are on the council's approved list; and
- A response plan was in place for security incidents such as the loss or theft of mobile devices.

1.29 However, we noted that:

- Approximately 70% of devices did not have the latest iOS operating system update, leaving them vulnerable to security incidents;
- The mobile phone and smart phone policy needs to be reviewed and should include the council's policy on other relevant mobile device security matters such as (but not limited to) bring your own device (BYOD) and installation of third party applications; and
- Password format rules on the MDM system need amending to bring it in line with the requirements of the council's IT security policy.

1.30 Actions were agreed with management to manage all of the findings identified.

LiquidLogic/CareFirst Application Audit (2019/20)

1.31 The LiquidLogic Adult Social Care System (LAS) is a key system within the council, used for recording and processing information relating to adult social care client care needs. This includes the management of contacts, referrals and support plans as well as recording safeguarding issues. The information held within LAS is particularly sensitive, including that which falls under the definition of 'special category data'.

1.32 Our audit evaluated the adequacy and effectiveness of the key configuration settings and access control mechanisms to a variety of sensitive processes in LAS, where there were risks associated with inappropriate and unauthorised access and/or processing. Such risks could potentially jeopardise effective care provision, and cause data protection issues and/or inappropriate use of information.

7

1.33 We were only able to provide Partial Assurance over the controls operating within the area under review because:

- New user accounts had been set up without management authorisation, and full access had been granted to some users prior to mandatory training occurring;
- Once users were set up, permissions were not routinely reviewed to identify any incorrect access or necessary changes;
- System changes and upgrade approvals were not always documented leading to a risk that the system may not have enough testing prior to go-live status; and
- A full disaster recovery test had not taken place since the implementation of the system.

1.34 Several areas of good practice were identified, including:

- Good communication took place with system users, including providing them with information around downtime, systems upgrades and changes via multiple channels; and
- Testing confirmed that controls were in place to ensure users were assigned appropriate permissions for their job role. System Administrator access was restricted to those who required it.

1.35 Unfortunately we were unable to provide assurance over ASC's Business Continuity arrangements in relation to LAS, as not all relevant documentation was able to be supplied to us ahead of the ASC's prioritisation of ongoing COVID-19 response activities.

1.36 Actions to address all of the issues identified during our audit have been agreed with management and these will be subject to a follow up by Internal Audit in due course to confirm appropriate implementation.

Digital Business & Insights Programme - 'As-Is' Process Assurance (2020/21)

1.37 The Digital Business & Insights Programme (DB&I) has been established to deliver transformation by either upgrading or replacing the council's existing SAP system. The DB&I Programme looks to

implement a new Enterprise Resource Planning (ERP) system, that will help the council's drive to deliver efficiencies through the transformation agenda.

1.38 The current SAP ERP system was implemented in 2004 and will no longer be supported beyond 2025. The overall cost of its replacement is expected to be circa £40m with the new system(s) expected to be implemented in 2021.

7

1.39 To support the programme, we undertook a review of the 'As Is' documentation of the system processes as it currently exists, to ensure that it accurately reflects the current control environment, thereby enabling any future changes to be identified, understood and formally assessed.

1.40 No formal report was produced from this review (and therefore no opinion given) as we fed back the findings from our work in real-time to enhance the programme documentation, leading to further improvements.

iPhone Refresh Project (2020/21)

1.41 The iPhone Refresh project is in the early stages of developing a detailed implementation plan for the deployment of new devices. IT&D sought advice from Internal Audit on its proposed approach to the collection of old devices.

1.42 We were able to provide advice and support to the process and advised on the appropriate mechanisms for formal decision-making. This advice has been included in revised plans and as a result no report was necessary at the conclusion of our work.

Other Audit Activity

Grant Claims

1.43 In the second quarter of 2020-21 we completed four grant certification audits on behalf of the council:

- Highways maintenance block funding and pot-hole repair capital grants from the Department for Transport - £23.67m;
- Urban Links to Landscape semester 4 (EU Interreg grant funding) - €26k (circa £23k);
- IMAGINE semester 3 (NE Europe grant funding) - €56k (circa £50k); and
- COVID-19 Bus Service Support Grant - £160k.

2 Covid-19 Response Work

2.1 The following paragraphs set out further details of the work that we have undertaken in providing advice and support to services in response to Covid-19. As reported to this Committee in our Quarter 1 Progress Report, as a result of the pandemic a significant proportion of our planned audit work in the first two quarters was paused so that we would not impede service response to the pandemic and, wherever possible, enable us to support this response.

7

COVID-19 Enquiries Standard Operating Procedure

2.2 The Programme Management Office (PMO) coordinated the council's approach to communication and enquiries relating to COVID-19 from people and partners with whom the council works, such as partner organisations, suppliers or providers, councillors, and MPs. General enquiries from members of the public requesting advice or assistance were handled by the Community Helpline and did not form part of this review.

2.3 The council had updated its Standard Operating Procedure (SOP), which sets out how information would be shared across the council and how enquiries should be managed and recorded. The PMO had produced a process note that sat alongside the SOP, intended to support officers managing enquiries or generating advice and guidance.

2.4 Individual directorates adopted their own approach to dealing with enquiries, partly to mitigate the potential bottleneck of the PMO dealing with all enquiries centrally, but also in recognition of local good practice already in place in some areas. The PMO requested that audit undertake a review of the arrangements in place to manage enquiries in order to:

- Establish and evaluate the processes in place for key, frontline services; and
- Assess compliance with processes where fully implemented.

2.5 Only a few services had a documented process and/or a record of enquiries specific to COVID-19. Only 5 of the 19 services we approached were aware of the corporate SOP and associated process note. Consequently, it was not possible to assess compliance with processes. The guidance was not passed on to officers responding to or maintaining records of COVID-19 enquiries. It is possible that the guidance went unnoticed due the focus being on ensuring continuity of services.

2.6 The efforts made by staff across the council to ensure the delivery of services during the COVID-19 pandemic is widely acknowledged. Whilst existing local methods of recording enquiries were

maintained by the services we tested, the inconsistent approach reduced strategic oversight of emerging issues or trends. Further, the council may face criticism or challenge if it is unable to evidence its response to COVID-19 enquiries.

2.7 On the basis of this finding we provided advice to the PMO about alternate ways to coordinate a corporate approach of this nature in the future. The PMO can now consider alternative arrangements should a second wave of COVID-19 or similar scenario occur in the future, especially as services may otherwise respond to further guidance in a similar manner.

7

3. Counter Fraud and Investigation Activities

3.1 Internal Audit deliver both reactive and proactive counter fraud services across the Orbis partnership. Work to date has focussed on the following areas:

National Fraud Initiative (NFI) Exercise

3.2 Internal Audit are currently working with the appropriate departments to ensure that the relevant datasets are uploaded for the next NFI exercise. The data is required to be uploaded by 1 December 2020 and the results from the exercise are due on 31 January 2021.

Fraud Response Plans

3.3 The Fraud Response Plans include a data analytics programme for key financial systems. Work on this programme (including creditors, debtors, payroll and pensions data) will commence in quarter three.

Fraud Awareness

3.4 Internal Audit has worked with the Blue Badge Team Manager to deliver fraud awareness training, and to develop a Misuse Response Plan to enable the team to respond in the most appropriate way to any allegations of fraud or misuse. In addition, we continue to monitor intelligence community alerts and the latest fraud bulletin is on the council's intranet.

Reactive Counter Fraud Work - Summary of Completed Investigations

Salary Overpayment

3.5 Following a routine audit of payroll, Internal Audit was notified that a leavers form for a member of staff who had left the council in November 2018 had not been processed until September 2019. As a result, the member of staff had continued to be paid their monthly wage creating an

overpayment of £14,608. Our investigation found that council had clear procedures around managing leavers, however, we found members of the team were not clear on certain of their responsibilities. This has now been addressed by the service, and the overpayment is in the process of being recovered.

7

Conflict of Interest

3.6 Internal Audit investigated an allegation of corruption in Children's Services. It was alleged that a member of staff had bypassed the competitive tendering process and had appointed their son-in-law to carry out work on behalf of SCC. The investigation found that there was no case to answer and that the relevant declaration and mitigations of risk were in place.

Surrey Fire & Rescue Service

3.7 Internal Audit undertook an investigation into an allegation relating to the purchase of drone services and an underwater camera for Surrey Fire & Rescue Service. The allegations included poor value for money, non-delivery of equipment and issues relating to potential conflicts of interest. The investigation found that the items had been purchased in line with Procurement Standing Orders and that there was no case to answer.

4. Action Tracking

4.1 All high priority actions agreed with management as part of individual audit reviews are subject to action tracking. All high-priority actions due to be implemented by management by the end of quarter two had at least been partially implemented.

4.2 High priority actions relating to the audit of Pension Fund Administration remain a work in progress in terms of their implementation, with revised dates for this agreed with management. Progress over full implementation will continue to be monitored and reported on by Internal Audit.

4.3 We are currently engaged in follow-up audits of Health and Safety, and of Surveillance Cameras, both of which have one previous high priority action associated with them. In both cases, the effect of the lockdown and Covid-19 had delayed the full implementation of actions, and once the follow-up audits are completed we will report the outcome to this Committee in due course.

5. Amendments to the Audit Plan

5.1 As referred to previously, a significant proportion of our planned work was paused in response to the pandemic. We have therefore revised and updated the audit plan for the remaining seven months of 2020/21 and will be presenting a separate report to this Committee as part of the November agenda papers.

7

6. Internal Audit Performance

6.1 In addition to the annual assessment of internal audit effectiveness against Public Sector Internal Audit Standards (PSIAS), the performance of the service is monitored on an ongoing basis against a set up agreed key performance indicators as set out in the following table:

Aspect of Service	Orbis IA Performance Indicator	Target	RAG Score	Actual Performance
Quality	Annual Audit Plan agreed by Audit Committee	By end April	**G**	Approved by Audit Committee on 22 May 2020 (April's committee was postponed due to COVID)
	Annual Audit Report and Opinion	By end July	**G**	2019/20 Annual Report and Opinion approved by Committee on 28 August (delayed due to COVID)
	Customer Satisfaction Levels	90% satisfied	**N/A**	No surveys received in the period
Productivity and Process Efficiency	Audit Plan – completion to draft report stage	90%	**N/A**	During the COVID-19 pandemic, the audit plan has been suspended to allow the organisation to respond to the emerging pandemic.
Compliance with Professional Standards	Public Sector Internal Audit Standards	Conforms	**G**	January 2018 – External assessment by the South West Audit Partnership gave an opinion of 'Generally Conforms' – the highest of three possible rankings June 2020 - Internal self-assessment completed, no major areas of non-compliance with PSIAS identified.

Aspect of Service	Orbis IA Performance Indicator	Target	RAG Score	Actual Performance
				June 2020 - Internal Quality Review completed, no major areas of non-compliance with our own processes identified.
	Relevant legislation such as the Police and Criminal Evidence Act, Criminal Procedures and Investigations Act	Conforms	G	No evidence of non-compliance identified
Outcome and degree of influence	Implementation of management actions agreed in response to audit findings	95% for high priority agreed actions	G	100%
Our staff	Professionally Qualified/Accredited	80%	G	92.9%[1]

[1] Includes staff who are part-qualified and those in professional training

Audit Opinions and Definitions

Opinion	Definition
Substantial Assurance	Controls are in place and are operating as expected to manage key risks to the achievement of system or service objectives.
Reasonable Assurance	Most controls are in place and are operating as expected to manage key risks to the achievement of system or service objectives.
Partial Assurance	There are weaknesses in the system of control and/or the level of non-compliance is such as to put the achievement of the system or service objectives at risk.
Minimal Assurance	Controls are generally weak or non-existent, leaving the system open to the risk of significant error or fraud. There is a high risk to the ability of the system/service to meet its objectives.

This page is intentionally left blank