# Appendix 1

## Audits Completed in Q2 (July to September)

### Annual Governance Statement

1.1 The Annual Governance Statement (AGS) is a statutory requirement for Local Authorities set out in the Accounts and Audit Regulations 2015. It is an accountability statement from the Council to stakeholders stating the arrangements in place to ensure compliance with its own code of governance on an annual basis, including how it monitors and evaluates the effectiveness of governance arrangements in the year, and on any planned changes in the coming period.

1.2 The Council's 2019/20 AGS was presented to, and approved by, the Governance Committee on 2 October 2020.

1.3 The purpose of this audit was to provide assurance that:

- The compilation and completion of the Annual Governance Statement adheres to the Accounts and Audit Regulations 2015;
- The Annual Governance Statement complies with the Local Code of Corporate Governance and is effectively communicated;
- The process for compiling the Annual Governance Statement is efficient, effective, and fit-for-purpose and information provided is accurate; and
- Agreed actions from the previous audit in 2014/15 have been implemented.

1.4 In completing this work, we found effective arrangements exist over the production of the AGS and were able to provide an opinion of **substantial assurance** as a result. Robust processes are in place to ensure the AGS adheres to the Accounts and Audit Regulations 2015 and there are effective procedures to evaluate, monitor and report on how the Council complies with the Local Code of Corporate Governance. Each Council department is required to identify actions to further strengthen governance arrangements.

1.5 A few minor issues for improvement were identified and these were agreed in full with management.

### Pension Fund Governance, Strategy and Investments

1.6 ESCC administers and manages the East Sussex Pension Fund (the Fund) on behalf of 134 employers. The Fund is responsible for managing assets for the long-term benefit of scheme members in accordance with statutory regulations. The Pension Committee is responsible for making arrangements for the administration of the Fund and its investments, receiving advice as appropriate from the Pension Board.

1.7 The Fund is a member of the ACCESS Pool, a collaboration of 11 Local Government Pension Scheme administering authorities who are working together to reduce investment costs and gain economies of scale. The ACCESS Pool was implemented in line with the 1 April 2018 deadline set by central government. It has a value of c. £46 billion, with the East Sussex Fund having invested £2.8 billion.

1.8 We reviewed the adequacy of governance arrangements over the ESPF, covering the strategy and the arrangements to manage investments, including pooling arrangements, to provide assurance that:

- Investments (inside and outside the ACCESS Pool) are well managed and that all income due is received promptly and intact;
- Governance arrangements provide sufficient and effective oversight;
- Risk management arrangements are robust;
- Communication is efficient and effective; and
- Accounting provides an accurate representation of the Fund's financial position.

1.9 In completing this work, we provided an audit opinion of **reasonable assurance**, finding that:

- Appropriate governance structures are in place, providing effective oversight and leadership. Meetings are held in accordance with the Council's Standing Orders and are minuted effectively. Both bodies' members are adequately qualified and knowledgeable in order to fulfil their roles;
- Investment performance is regularly reported to the Board and Committee and reviewed as appropriate;
- There is an independent advisor in place with the relevant knowledge and skills to support the Fund and its decision-making;
- Key risks are identified, reported and monitored; and
- Arrangements are in place to ensure appropriate communication takes place with employers and members.

1.10 Although we gave a reasonable assurance opinion, we identified areas for improvement, including:

- Ensuring the Pension Fund does not lend money to ESCC (the administering authority) accounts. We found two occasions where the Fund had lent money to ESCC, on a short-term basis, to prevent the ESCC bank account from becoming overdrawn. Records show that, whilst Pension Fund officers were aware of the transactions before they happened, there was no evidence of formal approval and no concerns were raised at the time that this was against Local Government Pension Scheme Regulations. The transactions did, however, follow normal ESCC treasury management processes, with approval from two members of the ESCC Treasury Management team on each occasion;
- The strengthening of governance arrangements within the ACCESS Pool, where there is a need (for the Pool) to agree and formalise a process to manage the performance of fund managers and investments, and to approve the governance manual that has been prepared but not yet implemented;

- Ensuring that external control assurance reports from fund managers are reviewed by Link Fund Solutions (the operator appointed to manage investments in the ACCESS Pool on a daily basis) to ensure that any known control weaknesses affecting investments are addressed, on a timely basis; and
- The need to reconcile records in SAP to those held by the Fund's custodian, more frequently.

1.11 A robust action plan has been agreed with management to address the findings of this review and the agreed actions for improvement are in progress.

**Property Asset Management System (PAMS) Replacement - Programme Governance and Risk Assessment**

1.12 The current Property Asset Management System (PAMS), Atrium, will no longer be supported from 2021. The system is used to hold asset management data on all Council property and operates as a works order management system for repair and maintenance. It also interfaces with the Council's current SAP ERP system.

1.13 The PAMS project sits under the Modernising Back Office Systems Programme (MBOS) and is governed by the MBOS Board, with a working group for PAMS in place under this. The PAMS project is focussed on transferring all functions carried out on Atrium onto a new asset management system. In addition, it will ensure that all property functions required to achieve a full holistic property management process are integrated and interfaced with the eventual SAP replacement.

1.14 The primary objective of this audit was to provide assurance that effective governance and risk management controls are in place for the PAMS project. In completing our work, we were able to provide an opinion of **substantial assurance** in this area because:

- Robust documentation for the PAMS project is in place, including a Business Case (which has been agreed at an appropriate level), a Project Initiation Document, Project Definition Document and Terms of Reference for the working group. This serves to outline key information in relation to the project, including its purpose and individuals to be involved;
- Governance arrangements for the project are appropriate and documented. Regular communication takes place with the MBOS board, including from the PAMS working group;
- Risks associated with the project are identified and assessed. These are assigned an owner, controls are identified, and the register is regularly updated to add, remove or reassess risks as appropriate;
- As the project progresses, stakeholder engagement is planned to increase and strategies around change management, quality management and closure of the project are due to be more fully refined.

1.15 One low risk action, aimed at making improvements to budgetary monitoring arrangements, was agreed with management.

**Data Analytics – Creditors**

1.16 The fraud threat posed during emergency situations, such as the Covid-19 global pandemic, is higher than at other times, and all public bodies should be attuned to the risks facing their organisations. A key objective of our work during the Covid-19 pandemic has been to support the organisation by reviewing major sources of data from within the Council for possible areas of fraud, error, duplicate payment or other suspicious activity. The primary objective of this work was to provide assurance that selected key controls, within Procure to Pay processes across the Council, were continuing to work effectively through the early stages of the Covid-19 pandemic. Using data analytics, the following areas were reviewed:

- Bank account changes to detect bank mandate fraud; and
- Payment trend analysis to identify potential overpayments.

Bank Account Changes

1.17 We undertook a data analytics exercise on vendor bank account changes made since lockdown and officers began working from home. This exercise involved identifying vendor accounts where changes had taken place and, on a cross-Orbis basis, completing a risk assessment of these in order to select the vendors and changes that we felt required further investigation. As part of the risk assessment, we sought to use a number of factors to influence our selection, including those where we felt it 'out of the ordinary' for companies to be making changes to their bank accounts at the time of a global pandemic (e.g. large multinational organisations or limited companies) and those which receive particularly high value and high volume payments. This cross-Orbis approach enabled the opportunity to share findings and intelligence for all partners and customers.

1.18 Throughout the investigation of these account changes, we did not identify any instances of potential fraud against the Council. However, opportunities to improve the control environment, particularly in relation to non-compliance with Council processes, were identified and improvements to processes agreed.

Payment Trends

1.19 Further analysis of payment trends against vendors was used to identify potential overpayments as a result of urgent payment requests. This work involved analysing average monthly spend against each vendor on a rolling 12-month basis, then selecting the top 20 increases, on both gross and percentage terms, for further investigation.

1.20 The investigation of these payments did not identify any potential overpayments as a result of fraud; however, an overpayment of £5,700 against one vendor in error was found. This was reported to the service area with subsequent action being taken to recover the funds.

1.21 It should be noted that the overpayment was identified after only a modest amount of time spent on the trend analysis. We concluded that it may therefore be cost effective for the Council to consider adopting and developing such an approach as part of its business as usual processes.

**Direct Payments for Adult Social Care**

1.22 Direct Payments are payments made directly to clients that allow them to choose and pay for support to meet the level of care required, which is based on an assessment of their needs. The legal framework for Direct Payments is set out in the Care Act 2014, Section 117(2C) of the Mental Health Act 1983 and the Care and Support (Direct Payments) Regulations 2014.

1.23 All clients are offered the option of a Direct Payment. Direct Payments are established through an Individual Service Agreement, which outlines the weekly amount paid by ESCC, and the amount that the client must contribute towards the cost of their care and support. Clients have the option to manage their own Direct Payment account or may choose to have the account managed by ESCC or an external service provider.

1.24 The Income and Payments Team transferred from Adult Social Care and Health (ASCH) to Business Operations, in May 2013. The administration of Direct Payments returned to Adult Social Care and Health in April 2019. On its return, ASCH recognised the need to strengthen controls and this need for improvement is reflected in some of the findings, below.

1.25 Since our work on this audit, up to and including February 2020, central government issued guidance in response to COVID-19 that superseded the Care Act (2014), resulting in the Direct Payments Team adapting and changing their working arrangements and processes, in order to accommodate the changed environment and statutory expectations. Additional testing of these revised, post Covid-19 processes, to meet the requirements of this government guidance, was not undertaken as part of this review, in order for the Direct Payments Team to focus their resources on their clients during this time.

1.26 The purpose of the audit was to provide assurance that:

- Amounts paid are correct and an appropriate level of care is received;
- Monies provided under the Direct Payment Scheme are used for their intended purpose;
- All client contributions are received; and
- Monies paid over to external Direct Payment providers are used to ensure that clients receive appropriate care, and excessive balances are not allowed to build up.

1.27 The needs assessment process, the calculation of direct payments and direct payments made through Children's Services were excluded from the scope of this review.

1.28 Based on our testing of the controls operating on Direct Payments, we gave an opinion of **partial assurance**, with some areas for improvement being identified, including the need to:

- Better monitor clients' Direct Payment account balances, where excessive balances were identified on some client accounts, and where we found that some balances had fallen below the permissible level on others, increasing the risk that clients do not receive the level of care that they have been assessed as needing, or that the Council is paying for care that is not required. It was acknowledged by management that this was an area that required improvement, and this may have been impacted, in part, by resourcing;
- Ensure there is a contractual requirement for external providers that manage clients' direct payments accounts, to review accounts' balances, as required under the Care and Support Regulation 2014;
- Ensure care plans are sufficiently clear to enable the Direct Payments Team to monitor account spend against care paid for, to ensure it is appropriate and, wherever possible, that transactions undertaken by clients on pre-paid cards contain enough information to allow analysis of the expenditure, so that any inappropriate use of funds can be identified; and
- Undertake annual reviews of all accounts in accordance with the requirements of the Care and Support Regulation (2014), where up to 40% of clients' accounts had not been reviewed, at the time of testing in February 2020, which may result in clients failing to receive care that meet their needs.

1.29 All of the above areas were discussed with management and appropriate actions to address them were agreed within a comprehensive management action plan. A formal follow-up review will be undertaken to assess the implementation of these.

1.30 It should also be noted, however, that several areas of good practice were identified as part of the review, as follows:

- Control over the creation of direct payment accounts is robust, as a signed and returned Individual Service Agreement (ISA) is in place prior to setting up each account;
- Payments to verified pre-paid card accounts are well controlled via four-weekly schedules, administered through ContrOCC;
- Clients are invoiced for their contributions; if these are not paid, there is an effective process in place to identify and chase payments owed; and
- Direct payment accounts are reconciled and closed promptly, once the client is no longer eligible to receive these payments.

**Patch Management**

1.31 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 hard and software following the application of a patch.

1.32 This 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 were reviewed within the recent Cyber Security audit (which we reported on in our Q1 progress report).

1.33 In completing our work, we were able to provide an opinion of **reasonable assurance** because:

- Patches are identified and deployed in a timely manner to relevant Council devices;
- Testing of patches and updates is robust for both laptop/desktop devices and sampled critical systems, serving to identify and allow correction of problems prior to wider rollout;
- Rollback arrangements are also in place should application of a patch have an adverse effect on system or hardware functionality; and
- Patches and updates are applied with consideration to balancing the benefits of patching against the risk of doing so, and the desire for user convenience.

1.34 Some opportunities to improve controls were also identified, however, including:

- The need to improve the governance arrangements in respect of patching, where reports on the Council's patching status are not routinely run or viewed by management. This could mean that any concerns over the effectiveness of the patch deployment are not escalated and managed, compromising the security of Council systems and data;
- Ensuring the IT Security and Safeguarding Policy, which includes patch management, is up-to-date and includes roles and responsibilities in relation to patching, and stipulates target times for patches to be applied; and
- The need to routinely identify, record and monitor end-of-life software, for which patches are no longer available, to ensure risks associated with these programmes being mitigated.

1.35 A formal action plan to address these areas was agreed with management.

**Cloud Computing**

1.36 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.

1.37 From a sample of four 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.

1.38 We were able to provide an audit opinion of **reasonable assurance** over the controls operating within the area under review because:

* IT&D have a robust risk assessment for evaluating the controls in place for systems, including specific reference to cloud management controls. Risks are identified and informed to the risk owner;
* A Data Protection Impact Assessment (DPIA) has been conducted for the systems which hold personally identifiable information;
* All system providers outline adherence to Data Protection legislation, including GDPR; and
* A Business Continuity Plan is in place for service areas using these systems.

1.39 There were, however, areas which required improvement, including in relation to ensuring there is always IT&D oversight prior to staff procuring and accessing cloud-based systems, so that formal risk assessments can be undertaken, risks appropriately managed and assurance sought that the provider has sufficient arrangements for business continuity, data security and access control. We found a lack of oversight, due to a combination of insufficient staff guidance around requesting use of such systems, a lack of technical controls to prevent access to unapproved cloud-based systems and the ease with which these systems can be procured and configured.

1.40 We also identified a need for system owners of cloud applications to fully understand the responsibilities of their role, which was not always the case. Whilst the expectations of a system owner for new systems and those which are reassessed have now been established and documented, existing system owners may still be unaware of their responsibilities.

1.41 For all of the findings of this audit, we have agreed actions to improve controls within a formal management action plan.

**Mobile Device Management**

1.42 Mobile devices such as smartphones and tablet computers have the capability to store large amounts of data and can present a high risk of data leakage and loss. In addition, devices are often valuable and are therefore attractive to theft and misuse.

1.43 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 the use of third-party software. The Council's MDM solution is provided by VMware AirWatch.

1.44 At the time of the audit, the Council's mobile device assets comprised of 3,172 smartphones and a small number of tablet computers.

1.45 This audit considered the Council's approach to managing the risks associated with the security and control of the data contained on, and security of, smartphones and tablets. The audit 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.

1.46 In providing an audit opinion of **reasonable assurance** in this area, we found:

- An appropriate MDM system is in place that enforces controls to help manage, monitor and secure mobile devices that access and/or store corporate data (including photos and footage) that may be of a sensitive or confidential nature;
- Security settings configured on the MDM system such as password rules, device encryption, data storage/backup, device inactivity etc. were found to be in line with common practice;
- Users of managed devices (devices that have been enrolled on to the MDM platform) are only granted access to a device via an authentication mechanism (e.g. use of passcode);
- Ability to install third party applications on managed devices has been restricted and users can only install applications that are on the Council's approved applications catalogue;
- A response plan is in place to respond to security incidents such as loss or theft of mobile devices; and
- The MDM system has the ability to lock or wipe managed devices remotely in the event of loss or theft.

1.47 Some areas for improvement were noted and agreed with management, including the need to update the mobile phone policy (which had originally been developed for traditional mobile devices with only basic telephony and messaging services and limited data storage and processing capabilities), and to ensure that devices no longer in use are monitored and action taken to cancel contracts as appropriate (at the time of the audit approximately £2k per month was being spent on mobile device contracts that had been inactive for over a year).

**Troubled Families**

1.48 The Troubled Families (TF2) programme has been running in East Sussex since January 2015 and is an extension of the original TF1 scheme that began in 2012/13. The programme is intended to support families who experience problems in certain areas, with funding for the local authority received from the Ministry of Housing, Communities and Local Government (MHCLG), based on the level of engagement and evidence of appropriate progress and improvement.

1.49 Children's Services submit periodic claims to the MHCLG to claim grant funding under its 'payment by results' scheme. The MHCLG requires Internal Audit to verify 10% of claims prior to the Local Authority's submission of its claim. We therefore reviewed 11 of the 111 families included in the July/September 2020 grant cohort.

1.50 In completing this work, we found that valid 'payment by results' (PBR) claims had been made and outcome plans had been achieved and evidenced. All the families in the sample of claims reviewed had firstly met the criteria to be eligible for the TF2 programme and had either achieved significant and sustained progress and/or had moved from out of work benefits into continuous employment. We therefore concluded that the conditions attached to the TF2 grant determination programme had been complied with.

**Department for Transport Grants**

**Capital Grants**

1.51 Well maintained highways not only improve local productivity but also the environment by reducing delays, and makes cycling, horse riding and walking more attractive. The Department for Transport (DfT) provides funding to highway authorities to ensure that our local roads and other highway assets are fit for the future.

1.52 The funding allocated to each local highway authority in England in is based on a formula using road length data provided by each local authority, and also takes into account the number of highways assets such as bridges and lighting columns for which they are each responsible for.

1.53 Grants paid to the Council may be used only for the purposes that a capital receipt may be used for in accordance with regulations made under section 11 of the Local Government Act 2003. Our work in this area concluded that the conditions attached to the following grant allocations had been complied with and a signed declaration was sent to the DfT by 30 September 2020:

- Integrated Transport Block;
- Highways Maintenance Block Needs Element;
- Highways Maintenance Block Incentive Element; and
- Pothole Action Fund and Flood Resilience Fund.

**Bus Service Operators Grant (BSOG)**

1.54 BSOG payments from the DfT are made to local authorities for running community transport and bus services. BSOG aims to benefit passengers by:

- Helping to keep fares down; and
- Enabling operators to run services that might otherwise be unprofitable and could lead to cancellation.

1.55 The BSOG grant is ring fenced and can be used to fund the provision of supported bus services or other related transport provision. Internal Audit are required to annually audit a sample of routes and payments to operators to ensure that payments are accurately calculated in-line with the formula provided by the DfT and that the conditions attached to the grant are complied with. This was all confirmed and a signed declaration was returned to the DfT within the required timescales.

**Covid-19 Bus Service Support Grant**

1.56 The nationwide lockdown imposed in March as a result of the COVID-19 pandemic led to a significant drop in patronage on public bus services. To support operators through this time of reduced income, the DfT released funding for Local Transport Authorities (LTA's) to distribute to tendered services that had been affected by, or needed to be adjusted because of, the impact of COVID-19.

1.57 The grant conditions required all bus operators in receipt of funding to provide between 40-50% of usual service capacity, or agree lower levels with the Local Authority in conjunction with the DfT, whilst Local Authorities were required to maintain contractual payments at normal levels throughout the funding period. Operators receiving the commercial element of the COVID-19 Bus Service Support Grant could not submit a claim for this LTA funding, and were required to confirm that no services would be double funded.

1.58 Internal Audit were required to confirm that the funding had been used in line with the grant conditions. Our testing concluded that the grant conditions had been met and that unused funding had been returned to the DfT as required.

**Blue Badge Grant**

1.59 In August 2019, an extension to the Blue Badge scheme came into force, allowing people with non-visible disabilities to apply for a Blue Badge. This change allows those with conditions such as dementia, epilepsy and Parkinson's to access a Blue Badge that would previously have been provided only for those with a physical disability. To support the implementation of the new criteria, the DfT provided Local Authorities with additional funding to be used to support expenditure lawfully incurred or to be incurred by them.

1.60 The conditions of this grant were non-specific and were interpreted as allowing the authority to utilise the funding to support the provision of Blue Badge services within the county. Analysis of the Blue Badge budget took place, and it was confirmed that an amount equivalent to the grant funding amount had been used to provide Blue Badge services. A confirmation letter was signed by the Chief Internal Auditor and Chief Executive, which was returned to the DfT by the deadline of 31st July 2020.

## 2. Counter Fraud and Investigation Activities

**Proactive Counter Fraud Work**

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

**National Fraud Initiative Exercise**

2.2 We are currently working with the appropriate departments to ensure that the relevant datasets are uploaded for the next National Fraud Initiative exercise. The results from the exercise are due on 31 January 2021.

**Counter Fraud Policies**

2.3 Each Orbis partner has in place a Counter Fraud Strategy that sets out their commitment to preventing, detecting and deterring fraud. We have reviewed the sovereign strategies to align with best practice and to ensure a robust and consistent approach to tackling fraud. These were approved by Audit Committee on 10 July 2020.

**Fraud Risk Assessments**

2.4 Fraud risk assessments are regularly reviewed to ensure that the current fraud threat for the Council has been considered and appropriate mitigating actions identified. We have updated the risk assessment to include new and emerging threats as a result of the COVID19 pandemic. This includes potential threats to payroll, staff frauds relating to home working and cyber frauds.

**Fraud Response Plans**

2.5 The Fraud Response Plans take into consideration the results of the fraud risk assessments and emerging trends across the public sector in order to provide a proactive counter fraud programme. The fraud response plans include an emphasis on data analytics. During the quarter, we developed a data analytics programme for key financial systems and work on this will continue in quarter three.

**Fraud Awareness**

2.6 The team are continuing to monitor intel alerts and the latest fraud bulletin is currently on the Council's intranet.

**Reactive Counter Fraud Work - Summary of Completed Investigations**

**Salary Overpayment**

2.7 We provided a team within Adult Social Care with support and advice following an allegation that an employee had claimed additional night hours. The employee had already received payment for these hours in their salary. The employee accepted a warning letter and the overpayment is in the process of being recovered.

**Schools** - Invoicing and Collection of Income at Breakfast Club

2.8 We investigated an allegation of irregularity in the management of invoicing and the collection of income at a Breakfast Club linked to a school. A report of our findings was issued to the school. The school held a disciplinary interview and the member of staff subsequently resigned from their extended roles.

**Schools** - Collection of Income for Swimming Pool

2.9 Following local press articles that a swimming pool had been closed despite the local community raising £100,000 towards its running over the last five years, we reviewed whether the money had been collected and had been banked appropriately.

2.10 No evidence was found to suggest any sums in the region of £100,000 had been raised by the local community to support the swimming pool and we therefore found no evidence to suggest any income had been misappropriated.

## 3. Action Tracking

3.1 All high priority actions agreed with management as part of individual audit reviews are subject to action tracking. There were two high-priority actions outstanding that were due to be implemented by management by the end of quarter two, both of which related to the Libraries Asset Management audit which was reported to Audit Committee in September this year. Revised dates for these have been agreed with management and progress over implementation will continue to be monitored and reported on.

## 4. Amendments to the Audit Plan

4.1 As previously reported, a significant proportion of our planned work was paused in response to the Covid-19 pandemic. It has therefore been necessary to prepare a revised audit plan for the remainder of the year, starting September 2020. Further detail on this can be found in our additional report to this meeting.

## 5. Internal Audit Performance

| Aspect of Service | Orbis IA Performance Indicator | Target | RAG Score | Actual Performance |
|---|---|---|---|---|
| Quality | Annual Audit Plan agreed by Audit Committee | By end April | G | Plan prepared for April approval, but formal reporting to Committee delayed due to Covid. Agreed by Committee on 13 May 2020. |
| | Annual Audit Report and Opinion | By end July | G | 2019/20 Annual Report and Opinion approved by Audit Committee on 10 July 2020. |
| | Customer Satisfaction Levels | 90% satisfied | G | 100%. |
| Productivity and Process Efficiency | Audit Plan – completion to draft report stage | 90% | N/A | During the Covid pandemic, the audit plan was suspended to allow the internal audit service to support the organisation's response. A revised audit plan has been developed from September and this target will be reported on from quarter 3 onwards. |
| 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.<br><br>June 2020 - internal self-assessment completed – no major areas of non-compliance with PSIAS identified. Internal quality review also 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. |

| Aspect of Service | Orbis IA Performance Indicator | Target | RAG Score | Actual Performance |
|---|---|---|---|---|
| Outcome and degree of influence | Implementation of management actions agreed in response to audit findings | 95% for high priority agreed actions | **R** | See Section 4 of this report. |
| Our staff | Professionally Qualified/Accredited | 80% | **G** | 90%[1] |

[1] Includes part-qualified staff and those undertaking 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. |