AVON & SOMERSET
POLICE & CRIME
COMMISSIONER

Enquiries to: #JAC **Telephone:** (01278) 646188

E-mail: JAC@avonandsomerset.pnn.police.uk **Date :** 11th March 2020

To: ALL MEMBERS OF THE JOINT AUDIT COMMITTEE

i. David Daw, Jude Ferguson (Chair), Zoe Rice, Martin Speller
ii. Chief Constable ("CC"), CFO for CC and Relevant Officers
iii. The Police & Crime Commissioner ("PCC")
iv. The CFO and CEO for the PCC
v. External and Internal Auditors

Dear Member

NOTICE OF MEETING

You are invited to a meeting of the **Joint Audit Committee** to be held at **11:00** on **19th March 2020** in the **Gordano Room, Police Headquarters, Portishead.** Due to the timing of this meeting lunch will be provided.

Joint Audit Committee Members are invited to attend a pre-meeting at 09:30 in the Gordano Room.

The agenda for the meeting is set out overleaf.

Yours sincerely

Alaina Davies
Office of the Police and Crime Commissioner

INFORMATION ABOUT THIS MEETING

(i) Car Parking Provision

Please follow the directions as you drive in. Follow the left lane for visitor parking

(ii) Wheelchair Access

The Meeting Room has access for wheelchair users. There are disabled parking bays in the visitor's car park next to reception. A ramp will give you access to reception, a lift is available to the 1st floor.

(iii) Emergency Evacuation Procedure

The attention of Members, Officers and the public is drawn to the emergency evacuation procedure for the **Gordano Room**: Follow the Green Fire Exit Signs to the **Visitor Car Park Assembly Point**.

(iv) Please sign the register.

(v) If you have any questions about this meeting, require special facilities to enable you to attend. If you wish to inspect Minutes, reports, or a list of the background papers relating to any item on this agenda, please contact:

Office of the Police and Crime Commissioner
Valley Road
Portishead
BS20 8JJ

Telephone: 01278 646188
Email: JAC@avonandsomerset.pnn.police.uk

(vi) REPORT NUMBERS CORRESPOND TO AGENDA NUMBER

AGENDA

19th March 2020, 11:00 – 14:00
Gordano Room, Police Headquarters, Portishead

1. **Apologies for Absence**

2. **Emergency Evacuation Procedure**
The Chair will draw attention to the emergency evacuation procedure for the **Gordano Room**: Follow the Green Fire Exit Signs to the **North Car Park Assembly Point**.

3. **Declarations of Gifts/Offers of Hospitality**
To remind Members of the need to record any personal interests or any **prejudicial interest** relating to the agenda and disclose any relevant receipt of offering of gifts or hospitality

4. **Public Access**

(maximum time allocated for this item is 30 minutes)

Statements and/or intentions to attend the Joint Audit Committee should be e-mailed to JAC@avonandsomerset.pnn.police.uk

Statements and/or intentions to attend must be received no later than 12.00 noon on the working day prior to the meeting.

5. **Minutes of the Joint Audit Committee Meeting held on 16th January 2020 (Report 5)**

6. **Internal Audit (Report 6):**
   a) **Internal Audit Plan 2020/21 and Internal Audit Charter**
   b) **Cybersecurity**
   c) **ICT Business Continuity**
   d) **Fleet Management**
   e) **Data Quality**
   f) **Refreshing Strategic Framework**
   g) **Personal Issue of Assets** (Final Draft)
   h) **Quarterly Update**

7. **Business from the Chair (Report 7):**
   a) **Police and Crime Board (Verbal Update)**
   b) **Update on IOPC Investigations (Verbal Update)**

8. **Office of the Police and Crime Commissioner Strategic Risk Register (Report 8)**

9. **Joint External Audit Plan (Report 9)**

10. **Summary of Recommendations (Verbal Update)**

Part 2
Items for consideration without the press and public present

11. Constabulary Strategic Risk Register (Report 11) – Paper to follow

POLICE AND CRIME COMMISSIONER FOR AVON AND SOMERSET **5**

MINUTES OF THE JOINT AUDIT COMMITTEE MEETING HELD ON THURSDAY 16TH JANUARY 2020 AT 11:00 IN THE CONFERENCE ROOM, POLICE HQ, VALLEY ROAD, PORTISHEAD

Members in Attendance
Jude Ferguson (Chair)
Sue Warman
Katherine Crallan
David Daw

New Members Observing
Martin Speller
Zoe Rice

Officers of the Constabulary in Attendance
Sarah Crew, Deputy Chief Constable
Nick Adams, Constabulary CFO
Dan Wood, Director of People and Organisational Development
Nick Lilley, Director of IT (part of the meeting)
Claire Hargreaves, Head of Finance (part of the meeting)
Superintendent Deryck Rees
Michael Flay, Governance Manager

Officers of the Office of the Police and Crime Commissioner (OPCC)
Mark Simmonds, OPCC CFO & Interim CEO
Ben Valentine, OPCC Strategic Planning and Performance Officer
Alaina Davies, OPCC Resources Officer

Also in Attendance
Jackson Murray, Grant Thornton
Iain Murray, Grant Thornton
Juber Rahman, SWAP
Laura Wicks, SWAP

36. Apologies for Absence

Sue Mountstevens, Police and Crime Commissioner
Andy Marsh, Chief Constable

37. Emergency Evacuation Procedure

The emergency evacuation procedure for the Conference room was noted.

38. Declarations of Interest / Gifts / Offers of Hospitality

None.

39. Public Access

There were no requests for public access

40. Minutes of the Joint Audit Committee Meeting held on 25th September 2019 (Report 5)

RESOLVED THAT the minutes of the meeting held on 25th September 2019 were confirmed as a correct record and signed by the Chair.

Action update:

Minute 31b(i) Scheduling of a future Health and Safety audit has been discussed. **Close Action**

Minute 31b(ii) The Joint Audit Committee Terms of Reference are being updated and will be discussed at the March 2020 meeting of the Joint Audit Committee.

Minute 31a(i) The final Workforce Plan internal audit report is included in the papers for this meeting at item 7a. **Close Action**

Minute 31a(ii) Will agree a timeline to look at Workforce Planning in 12-18 months with the report presented today being used as a baseline.

Minute 31a(iii) The Internal Auditors compared the timeline for audits against what else is happening in the organisation to ensure delivery is realistic. **Close Action**

Minute 32a Amendments to the Annual Audit letter, as discussed at the last meeting of the Joint Audit Committee, were made and the updated version published. **Close Action**

41. Business from the Chair

a) General Updates

The Chair gave a general update on changes in personnel. The PCC has announced that she will not be standing for PCC again in the upcoming PCC election in May 2020. The OPCC CEO has now left and has announced that he will be standing for PCC in the upcoming election. The OPCC CFO has agreed to take on the CEO role as an interim measure for 9 months. The Constabulary CFO has agreed to take on the role on Section 151 officer for the OPCC as the CEO cannot carry out this role. It was noted that purdah for the PCC election begins on 23rd March 2020.

The Chair welcomed new Joint Audit Committee (JAC) Members, Martin Speller and Zoe Rice, who will be taking up their roles for the

March 2020 Joint Audit Committee meeting. It was noted that David Daw, current Member, has been appointed for a full term.

The Chair thanked JAC Members Katherine Crallan and Sue Warman for their work over two terms (each 3 years) plus an additional year. These Members were fundamental in developing what was a new Committee. This is their last meeting.

The updated JAC Terms of Reference will be formally presented to the Joint Audit Committee for discussion at the March 2020 meeting.

b) Police and Crime Board

JAC Members receive updates from the OPCC CFO & Interim CEO on discussions of the Police and Crime Board (PCB). Highlights of discussions from the PCB over the last quarter include:

- The rolling assurance programme which has been open and engaging.
- Uplift (Futures Programme) – the PCB is moving from scrutiny during a time of austerity to scrutiny of an expanding organisation. Communication and managing public expectation regarding when additional resources will be operational is key.
- PCC election – the OPCC will need to understand the mandates of candidates and how this will translate to the development of a new Police and Crime Plan.
- Underspend – the underspend in the overall budget reported at the end of Quarter 1 has reduced following investment in change and uplift. The remaining amount will be transferred to Reserves at the financial year-end for investment in Capital projects.
- 2020/21 Funding Settlement – the delay in the announcement of the funding settlement is a risk to the organisation. The timescales for finalising the Medium Term Financial Plan are very tight as a consequence. The announcement is now not expected until 23rd January 20 and the report is due to be presented to the Police and Crime Panel on 4th February 20 for approval. All PCCs are in the same position with regard to this risk. The Constabulary have modelled a range of options with different precept levels in order to be as prepared as possible.
- Major Projects – Force Futures (Uplift) is going to be the major project for the Constabulary which will require a lot of organisational support. IT redesign is not yet complete and the Constabulary are keeping track of National IT Projects. Estates updates have been given.
- Scrutiny of HR – the recruitment trajectory is presented at each PCB. The focus is on ensuring the Constabulary have the right people for the future of the organisation.

c) Update on Independent Office for Police Conduct (IOPC) Investigations

An update was given on the 14 IOPC investigations relating to incidents occurring between June 2018 and January 2020. Cases are referred to the IOPC for a number of reasons including Abuse of Power, Taser deployment, excess use of force, death following police contact and corruption. Members were assured that the working relationship with the IOPC is good and that Avon and Somerset is not an outlier in terms of the number of cases referred. Learning is taken from each of the cases. The advantage of Body Worn Video cameras was discussed and the effect of this technology on timely completion of investigations.

42. Internal Audit Reports (Report 7):

a) Workforce Plan

A partial audit assurance opinion was given on workforce planning as a reflection of the ongoing nature of this piece of work which is still in its infancy - positive progress is being made. This report provides a baseline going forward. It was noted that there were communication issues between the Constabulary and the Internal Auditors in terms of information requested being provided in a timely manner and giving clear evidence of activities taking place – the learning from this will be taken forward. Members encouraged Internal Audit and Constabulary People and Organisational leads to liaise regarding communication as part of new ways of working and agree how to best share information and initiatives relevant to audit. Members thanked the Internal Auditors for the content, clarity and format of the report.

Members queried the timescale for procurement and introduction of the new learning management system (Chronicle) and the e-recruitment system.

Implementation of the e-recruitment system will begin this month for staff and run parallel to the old system to start with as the Constabulary cannot jeopardise the recruitment of officers through the use of a new system. Once fully implemented this system will provide a seamless end to end experience for candidates which will help with attraction, efficiency and timeliness. This system will also aid management of the HR function and availability of management information.

Members were assured that there has been significant progress in terms of Chronicle and implementation of this should begin in the next 2-3 months. The Constabulary currently have many systems in place to record the skills, competency and qualifications of staff and officers so having this one system will make a huge difference to facilitating better workforce planning and training.

It was noted that the Constabulary have achieved much in the context of managing business as usual at the same time as the uplift (going from an organisation recruiting 70-80 officer per year to 360). The Director of People and Organisational Development has now left and the Deputy has taken on this role in the interim. During this time the

Constabulary also took staff back in-house from South West One (SW1).

Members raised concerns regarding the diversity opinion given in the report. The Constabulary assured Members of the activities taking place which had not clearly been conveyed to the Internal Auditors. There is a holistic plan in place which is discussed at quarterly Diversity and Inclusion Boards. The Board is driving the Constabulary vision of being the most inclusive force in the UK. Outreach work continues along with engagement, training and development in relation to diversity. The Board monitors progress of the 5 key initiatives. The Constabulary had a detailed review by the National Equality Standard which was positive. It was noted that diversity information from recruitment could have been better explained – uplift in each area of diversity with recent recruitment is a positive indicator that this work is starting to have an impact. Inclusion is at the centre of the Strategic Framework. Diversity data is reported to PCB and Members were assured that there is a list of Diversity Champions. The Deputy Chief Constable invited Joint Audit Committee Members to observe a Diversity and Inclusion Board.

Members noted that the Constabulary is an organisation with high aspirations and were assured that work in this area is beginning to have an impact. It was noted that the HMICFRS PEEL inspection on Future Plans is yet to be published.

The Constabulary and Internal Auditors will agree the best time to undertake a further audit of this area of work.

Resolved that the Constabulary and Internal Auditors will agree the best time to carry out a further audit on Workforce Planning.

b) Payroll and Expenses

A reasonable audit assurance opinion was given on Payroll and Expenses. This was a helpful report which gives good areas of focus for improvement. The Constabulary notes the points raised but highlighted the difficulty with some of the recommendations e.g. ensuring VAT receipts are retained for each Corporate Card transaction.

The Constabulary accept the recommendations regarding ensuring all members of staff have a signed contract of employment which is retained by the organisation. They also accept the recommendation regarding ensuring that line managers inform payroll in a timely manner of those leaving the organisation in order to avoid overpayments being made in error.

Members queried whether the Internal Auditors benchmarked against other forces in their observations of the use of procurement cards and prevention of fraud. The internal auditors looked for obscure transactions e.g. casino payments. In some cases descriptions of spend had been left blank and therefore assurance cannot be given on these payments. The Constabulary CFO assured Members that checks on the use of procurement cards are carried out – only 25 cards are currently issued in total across the organisation with tight controls on the use of these. The cards are issued by Nat West with tight banking controls and limited use on what can be purchased. Secondary approval is required on the monthly returns for spend on these cards.

c) Overtime Payments

A partial audit assurance opinion was given on Overtime Payments. It was noted that wellbeing issues were identified during testing and recommendations were made as a result. The Constabulary is looking at an automated system for paying overtime which has not been claimed manually within set time parameters.

The overspend on overtime was discussed. Members were informed that much of this relates to mutual aid requests, which is offset by income the Constabulary cannot budget for. Members were assured that the Constabulary are confident in the level of control around this.

The wellbeing concerns in relation to overtime are noted by the Constabulary and further analysis will be taken forward through the Senior Leadership Team.

Members queried whether the timelines for actions in response to these recommendations could be shorter. The Constabulary are looking at automation and as such require the time to explore the options, carry out consultation and implement changes.

d) Personal Issue of Assets

Personal Issue of Assets is a draft report which will be presented as a final report at the March meeting of the Joint Audit Committee. This is an area the Constabulary were keen for the Internal Auditors to look at in the context of it being a new area of risk with the return of the function following the end of the South West One contract.

Members raised concerns regarding the number of staff and officers who have not yet completed the data protection e-learning. The Constabulary are working on tightening up compliance around completing the National Centre for Applied Learning Technology (NCALT) training.

The Constabulary has seen a massive growth in the personal issue of assets with the introduction of mobile working. This means there is an increased reliance on the personal issue of assets. Staff are not expected to wait for their devices to be fixed in cases of failure of equipment and are instead being issued with new ones to ensure they can continue to work.

The Strategic Information Management Board was re-established a year ago to reflect the risks in this area. The Board monitors training. It was noted that a tool is to be launched which will be a prompt to read relevant policies and ensure compliance.

The Constabulary accept all of the recommendations in the report and have completed some actions in response to these this week. Some of the actions will take longer to close e.g. introduction of the tooling support.

The Director of IT also highlighted that he recently carried out a reconciliation of Body Worn Video (BWV) cameras and will address any issues through policy.

e) Accounts Payable

A partial audit assurance opinion was given in relation to Accounts Payable. One recommendation relates to checking the correct VAT registration number of a new supplier. Actions are needed to resolve the case found in the system where an incorrect number had been provided by the supplier. The Constabulary are taking steps to resolve the issue identified and will ensure that they check the validity of numbers supplied going forward.

A recommendation was also made about duplicate suppliers on the system. In some cases suppliers might appear to be duplicates but aren’t e.g. where a large company is set up on the system who also have a local franchise on the system.

Members were assured that no duplicate payments were identified during the audit.

f) Quarterly Update

The report gives an update on activities in the previous quarter and year to date. There are five assurance pieces of work left to be completed. Many of the reports with a partial assurance opinion to date were borderline between partial and reasonable. The scoping of the Strategic Framework audit will be carried out next week.

43. External Audit Update (Report 8)

Members were informed that Jackson Murray has accepted a promotion to Director. The new external audit manager will be Gail Turner-Radcliffe and she will attend the March 2020 Joint Audit Committee meeting.

The Audit Plan will be submitted to the March 2020 Joint Audit Committee meeting. Following the concerns raised around the late increase in fees for the previous year the External Auditor will write to the Constabulary CFO and OPCC CFO & Interim CEO regarding a further increase this year. Fees are increasing and this is a trend across the audit market as a result of increased regulations and pressure from the Financial Reporting Council (FRC). There is a repositioning of external audit and what it is required to undertake which is impacting fees. This will be discussed further at the next meeting of the Joint Audit Committee.

The External Auditors are running some national training events for JACs. It was agreed that a local event should be run for the South West in the spring. The focus will be the future of local audit, changes to the National Audit Office (NAO) and the current review of audit activities. Members would like training to cover the broad makeup of the accounts.

The JAC Chair, Constabulary CFO and OPCC CFO & Interim CEO have contributed to the national review work with comments regarding the usefulness of the VFM work and also the relevance of going concern. It is proposed that the VFM section will not form part of the report in future and will instead be included as narrative in the Annual Audit Letter without an opinion.

Resolved that the External Auditors should work with the OPCC on the arrangements for running a South West JAC event.

44. Office of the Police and Crime Commissioner Strategic Risk Register (Report 9)

It was noted that there are a number of risks associated with the Constabulary and OPCC sharing a Section 151 officer. This has been agreed as an interim measure and the OPCC is confident this can work due to the trust and confidence it has in the Constabulary CFO. Although the OPCC would not wish for this to be a permanent option due to the need for independence it was noted that this is how some OPCCs are set up. This will be resolved by the end of the calendar year once the new PCC has taken up the role.

The OPCC CFO has taken on the role of CEO on an interim basis for 9 months which creates capacity risks within the OPCC. The PCC and OPCC Senior Leadership Team (SLT) have agreed a plan to divide responsibilities and put in place an OPCC Management Board – these actions mitigate strategic risk 6.

As a result of the above Strategic Risk 1 (Governance Failure) and Strategic Risk 6 (Lack of Capacity/ Capability within the OPCC) have increased. Members were assured that there are controls in place to mitigate these risks.

The effect on the strategic risks of the PCC’s decision not to stand again for PCC in the upcoming election was discussed. This does create uncertainty which will need to be reflected. The OPCC only know of two confirmed candidates so far and are in touch with the Police Area Returning Officer (PARO) to confirm when the final date by which candidates must confirm will be – until this date the OPCC can’t carry out environmental scanning. There will be a specific risk of the new PCC coming into the role with the old Police and Crime Plan, as it will take time for a new plan to be written.

The OPCC will equip candidates with as much information as possible to help them form a realist view of the role and ensure a well-informed pool of candidates. It was noted that the PCC Election Microsite is already up and running.

The governance of policing going forward was discussed and the role of the PCC in the National Policing Board – local priorities versus the national deliverables. This has been discussed at PCB.

45. Constabulary Strategic Risk Register (Report 10)

The Governance Manager informed Members of his intention to carry out some testing around mitigating actions. At the March Joint Audit Committee a high level mapping of what is being assured, what the risks are, areas for future scrutiny and how this relates to strategic objectives will be discussed.

The Constabulary will consider whether they need a specific risk around failure to deliver the Police and Crime Plan as this drives everything they do. Also consideration will be given as to whether collaborations is a strategic risk.

Information governance and the quality of information is a concern and the Constabulary are implementing changes to improve this e.g. system changes (compliance by design), process automation to identify duplicates. Data quality training is underway but improvement is slow. The Constabulary is recognised as outstanding in terms of analytics. The Constabulary received a visit from the Information Commissioners Office and they gave positive feedback and saw the work being done as pioneering – this gives assurance the Constabulary are on the right path. Avon and Somerset are not different to other forces in the challenges faced in this area of business but have chosen to highlight it. Innovation in an organisation exposes risk but leads to improvements being made

Business continuity was raised by Members. The Business Continuity audit report will be presented at the March 2020 Joint Audit Committee meeting. Members were assured that the Communications Disaster Recovery function has now been moved from the old Taunton Police station to Bridgwater and the Constabulary will test this.

Underspend on the budget was raised. Funding has been allocated in-year to projects and the residual amount will be transferred to reserves at the financial year-end to fund capital projects. The latest underspend figure reported at the end of Quarter 3 is £3.3m.

46. Summary of Recommendations (Verbal Update)

Since 2017 to date the Constabulary have received 140 recommendation from Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) of which 110 are complete, 28 in progress and 2 are overdue. One of the overdue recommendations relates to fraud and the Constabulary awaits national guidance regarding cyber-crime in order to complete this. The other overdue recommendation which relates to the Professional Standards Department (PSD) and vetting should be complete by the end of March 2020.

Since 2017 to date the Constabulary have received 149 Internal Audit recommendations of which 134 are complete, 15 are in progress and none are overdue.

The meeting concluded at 13:30

CHAIR

UNCONFIRMED Draft

ACTION SHEET

MINUTE NUMBER	ACTION NEEDED	RESPONSIBLE MEMBER/ OFFICER	DATE DUE
Minute 31b(ii) **Internal Audit: Quarterly Update** **25th September 2019**	The Joint Audit Committee Terms of Reference will be reviewed prior to the next Joint Audit Committee meeting and be submitted for discussion at that meeting.	OPCC CFO/ OPCC Strategic Planning and Performance Officer/ Head of Improvement	March 2020
Minute 42a **Internal Audit: Workforce Plan** **16th January 2020**	The Constabulary and Internal Auditors will agree the best time to carry out a further audit on Workforce Planning	Director of People and Organisational Development	TBA
Minute 43 **External Audit Update** **16th January 2020**	The External Auditors should work with the OPCC on the arrangements for running a South West JAC event.	Grant Thornton/ OPCC	Immediate

6a

Avon & Somerset Police and the Office of the Police and Crime Commissioner (OPCC)

Proposed 2020-21 Internal Audit Plan and Internal Audit Charter

Internal Audit ▪ Risk ▪ Special Investigations ▪ Consultancy

Unrestricted

The Internal Audit Plan: Summary

The internal audit plan represents a summary of the proposed audit coverage that the internal audit team will deliver throughout the 2020/21 financial year.

Delivery of an internal audit programme of work that provides sufficient and appropriate coverage, will enable us to provide a well-informed and comprehensive year-end annual internal audit opinion.

Introduction and Objective of the Internal Audit Plan

Internal audit provides an independent and objective opinion on the Force's and OPCC's risk management, governance, and control environment by evaluating its effectiveness.

Prior to the start of each financial year, SWAP, in conjunction with senior management, put together a proposed plan of audit work. The objective of our planning process and subsequent plan is to put us in a position to provide a well-informed and comprehensive annual audit opinion, based on sufficient and appropriate coverage of key business objectives, associated risks, and risk management processes.

The outcomes of each of the audits in our planned programme of work, will provide senior management and Members with assurance that the current risks faced by the Force and OPCC in these areas are adequately controlled and managed.

It should be noted that internal audit is only one source of assurance, and the outcomes of internal audit reviews should be considered alongside other sources, as part of the 'three lines of defence' assurance model. Key findings from our internal audit work should also be considered in conjunction with completion of the Annual Governance Statement for the Force and OPCC.

It is the responsibility of the Force's and OPCC's respective leadership teams and the Joint Audit Committee (JAC), to determine that the audit coverage contained within the proposed audit plan is sufficient and appropriate in providing independent assurance against the key risks faced by the organisation.

When reviewing the proposed internal audit plan (as set out in Appendix 1), key questions to consider include:

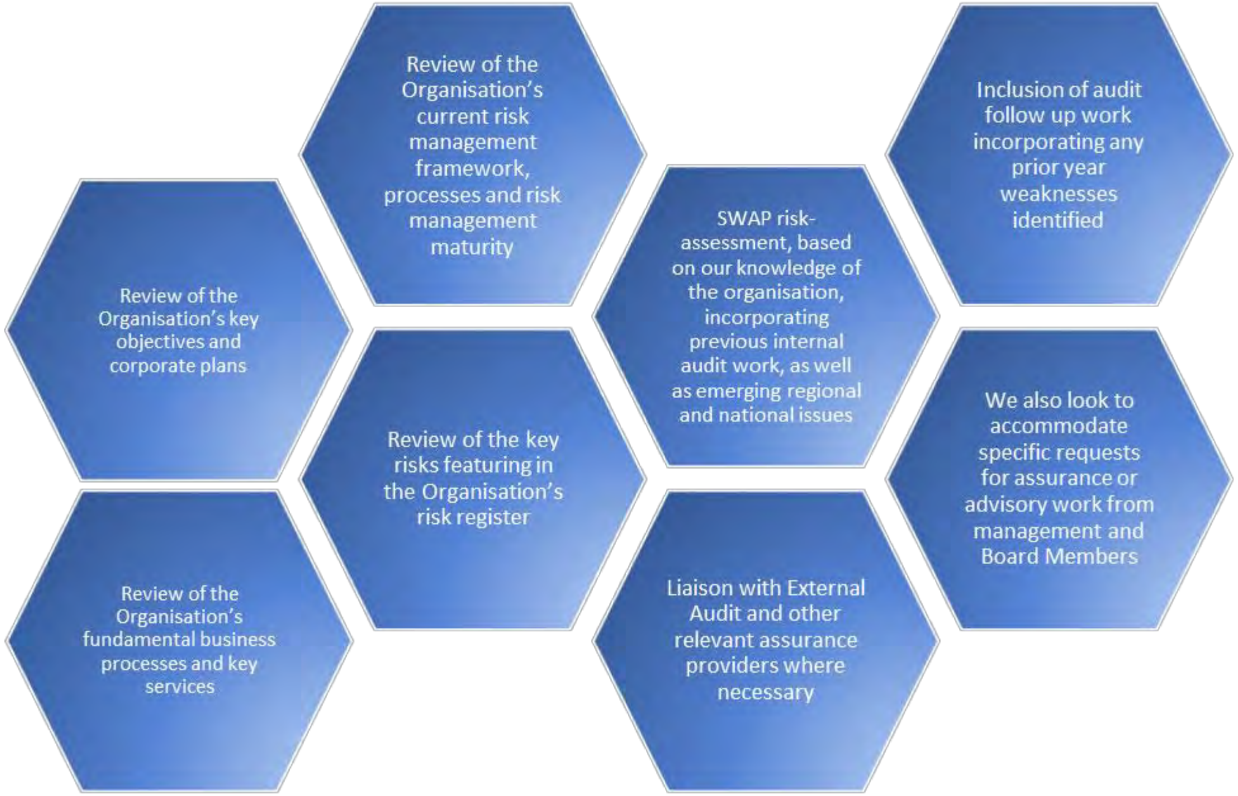
- Are the areas selected for coverage this coming year appropriate?
- Does the internal audit plan cover the organisation's key risks as they are recognised by the senior leadership teams of the Force and OPCC and the JAC?
- Is sufficient assurance being received within our annual plan to monitor the organisation's risk profile effectively?

The Internal Audit Plan: Approach

To develop an appropriate risk-based audit plan, SWAP have consulted with senior management, as well as reviewing key documentation, in order to obtain an understanding of the organisation's strategies, key business objectives, associated risks, and risk management processes.

Approach to Internal Audit Planning 2020/21

The factors considered in putting together the 2020/21 internal audit plan have been set out below:



Review of the Organisation's key objectives and corporate plans

Review of the Organisation's fundamental business processes and key services

Review of the Organisation's current risk management framework, processes and risk management maturity

Review of the key risks featuring in the Organisation's risk register

SWAP risk-assessment, based on our knowledge of the organisation, incorporating previous internal audit work, as well as emerging regional and national issues

Liaison with External Audit and other relevant assurance providers where necessary

Inclusion of audit follow up work incorporating any prior year weaknesses identified

We also look to accommodate specific requests for assurance or advisory work from management and Board Members

We will regularly re-visit and adjust our programme of audit work to ensure that it matches the changing risk profile of the organisation's operations, systems and controls. Whilst there is no formal contingency allocation, our 2020/21 audit plan can remain flexible to respond to new and emerging risks as and when they are identified.

The Internal Audit Plan: Risk Assessment

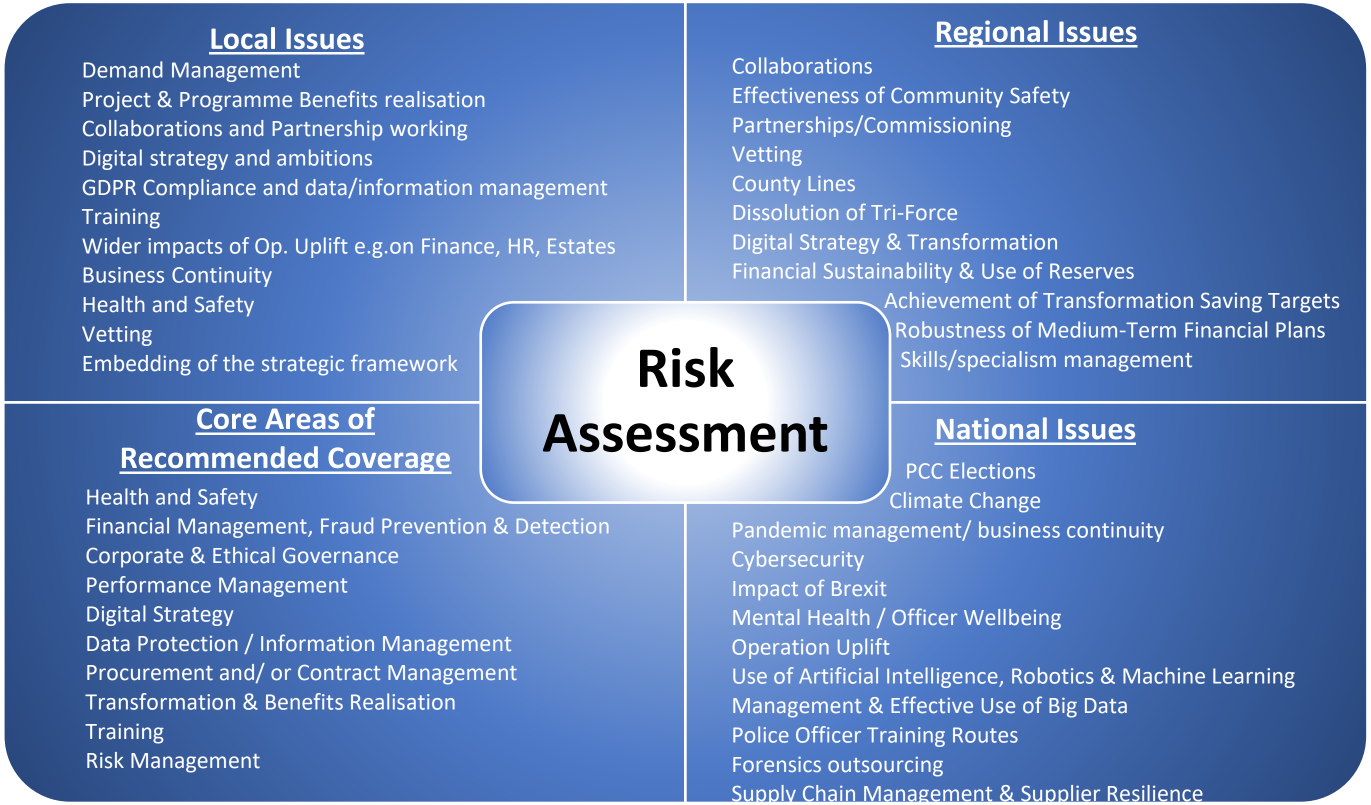
A documented risk assessment prior to developing an internal audit plan, ensures that sufficient and appropriate areas are identified for consideration.

As above, it is the responsibility of the leadership teams for the Force and OPCC and the JAC to ensure that, following our risk assessment, the proposed plan contains sufficient and appropriate coverage.

Internal Audit Annual Risk Assessment

Our 2020/21 internal audit programme of work is based on a documented risk assessment, which SWAP will re-visit regularly, but at least annually. The input of senior management as well as review of the risk registers for the Force and OPCC will be considered in this process.

Below we have set out a summary of the outcomes of the risk assessment for the Force and OPCC:



Risk Assessment

Local Issues

Demand Management
Project & Programme Benefits realisation
Collaborations and Partnership working
Digital strategy and ambitions
GDPR Compliance and data/information management
Training
Wider impacts of Op. Uplift e.g.on Finance, HR, Estates
Business Continuity
Health and Safety
Vetting
Embedding of the strategic framework

Regional Issues

Collaborations
Effectiveness of Community Safety
Partnerships/Commissioning
Vetting
County Lines
Dissolution of Tri-Force
Digital Strategy & Transformation
Financial Sustainability & Use of Reserves
Achievement of Transformation Saving Targets
Robustness of Medium-Term Financial Plans
Skills/specialism management

Core Areas of Recommended Coverage

Health and Safety
Financial Management, Fraud Prevention & Detection
Corporate & Ethical Governance
Performance Management
Digital Strategy
Data Protection / Information Management
Procurement and/ or Contract Management
Transformation & Benefits Realisation
Training
Risk Management

National Issues

PCC Elections
Climate Change
Pandemic management/ business continuity
Cybersecurity
Impact of Brexit
Mental Health / Officer Wellbeing
Operation Uplift
Use of Artificial Intelligence, Robotics & Machine Learning
Management & Effective Use of Big Data
Police Officer Training Routes
Forensics outsourcing
Supply Chain Management & Supplier Resilience

The Internal Audit Plan: Coverage

Following our SWAP Risk Assessment above, we have set out how the proposed 20/21 plan presented in Appendix 1 provides coverage of the key components set out in the Force Management Statement (FMS).

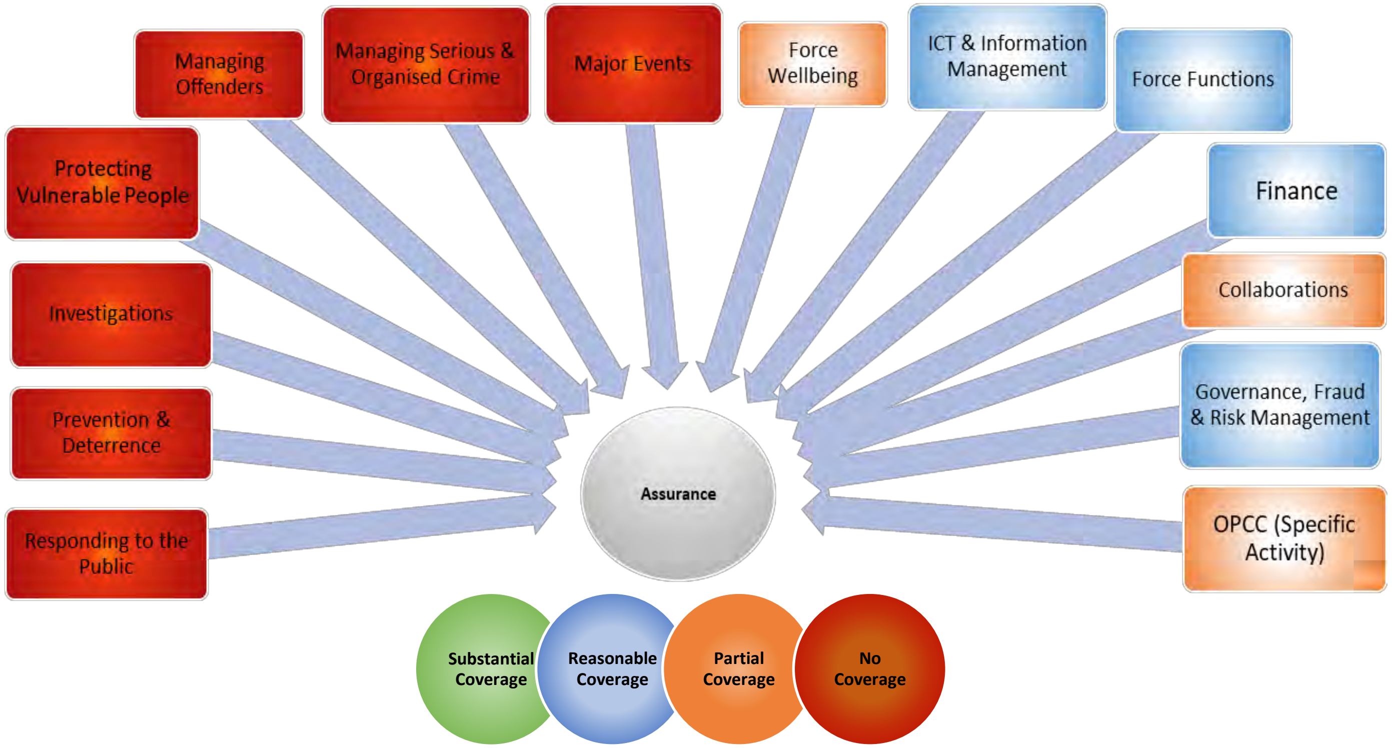
We have taken the approach of aligning our Audit universe with the Force Management Statements from HMICFRS as these will be used to inform their risk-based testing as part of the updated approach to PEEL Reviews. This will assist senior management and Members with identifying where gaps in assurance may exist.

Internal audit is only one source of assurance; therefore, where we have highlighted gaps in our coverage, assurance should be sought from other sources where possible in order to ensure sufficient and appropriate assurances are received.

For those areas marked as Red (No Coverage), we anticipate that other assurance providers, such as HMICFRS, will be covering those areas.

Internal Audit Coverage in 2020/21

Following our SWAP risk assessment, we have set out below the extent to which the proposed plan presented in Appendix 1 provides coverage of the key corporate objectives and risks for the Force and OPCC, as well as our core areas of recommended audit coverage:



Internal audit coverage can never be absolute and responsibility for risk management, governance and internal control arrangements will always remain fully with management. As such, internal audit cannot provide complete assurance over any area, and equally cannot provide any guarantee against material errors, loss or fraud.

The Internal Audit Plan: SWAP

SWAP Internal Audit Services is a public sector, not-for-profit partnership, owned by the public sector partners that it serves. The SWAP Partnership now includes 24 public sector partners, crossing eight Counties, but also providing services throughout the UK.

As a company, SWAP has adopted the following values, which we ask our clients to assess us against following every piece of work that we do:

- **Candid**
- **Relevant**
- **Inclusive**
- **Innovative**
- **Dedicated**

Your Internal Audit Service

Audit Resources

The 2020/21 internal audit programme of work will be equivalent to 180 days. The current internal audit resources available represent a sufficient and appropriate mix of seniority and skill to be effectively deployed to deliver the planned work. The key contacts in respect of your internal audit service for Avon and Somerset Police and OPCC are:

Laura Wicks, Assistant Director – laura.wicks@swapaudit.co.uk, 01935 848540
Ed Nichols, Principal Auditor – edward.nichols@swapaudit.co.uk, 01935 848540
Juber Rahman, Senior Auditor – juber.rahman@swapaudit.co.uk, 01935 848540

External Quality Assurance

SWAP work is completed to comply with the International Professional Practices Framework of the Institute of Internal Auditors (IPPF).

Every three years, SWAP is subject to an External Quality Assessment of Internal Audit Activity. The last of these was carried out in February 2020 which confirmed general conformance with the IPPF.

Conflicts of Interest

We are not aware of any conflicts of interest within Avon and Somerset Police and OPCC that would present an impairment to our independence or objectivity. Furthermore, we are satisfied that we will conform with our IIA Code of Ethics in relation to Integrity, Objectivity, Confidentiality, & Competency.

Consultancy Engagements

As part of our internal audit service, we may accept proposed consultancy engagements, based on the engagement's potential to improve management of risk, add value and improve the organisation's operations. Consultancy work that is accepted, will contribute to our annual opinion and will be included in our plan of work.

Approach to Fraud

Internal audit may assess the adequacy of the arrangements to prevent and detect irregularities, fraud and corruption. We have dedicated counter fraud resource available to undertake specific investigations if required. However, the primary responsibility for preventing and detecting corruption, fraud and irregularities rests with

Over and above our internal audit service delivery, SWAP will look to add value throughout the year wherever possible. This will include:

- **Pieces of regional audit work with coverage directed by the Regional Directors of Finance**
- **Regional Police Bulletins twice per year detailing areas of risk identified within audit work**
- **Benchmarking and sharing of best-practice between our public-sector Partners**
- **Regular newsletters and bulletins containing emerging issues and significant risks identified across the SWAP partnership**
- **Communication of fraud alerts received both regionally and nationally**
- **Annual Member training sessions**

management who should institute adequate systems of internal control, including clear objectives, segregation of duties and proper authorisation procedures.

Our Reporting

A summary of internal audit activity will be reported quarterly to senior management and the Joint Audit Committee. This reporting will include any significant risk and control issues (including fraud risks), governance issues and other matters that require the attention of senior management and/or the Audit Committee. We will also report any response from management to a risk we have highlighted that, in our view, may be unacceptable to the organisation.

Internal Audit Performance:

As part of our regular reporting to senior management and the JAC, we will report on internal audit performance. The following performance targets will be used to measure the performance of our audit activity:

Performance Measure	Performance Target
Delivery of Annual Internal Audit Plan Completed at year end	>90%
Quality of Audit Work Overall Client Satisfaction *(did our audit work meet or exceed expectations, when looking at our Communication, Auditor Professionalism and Competence, and Value to the Organisation)*	>95%
Outcomes from Audit Work Value to the Organisation *(client view of whether our audit work met or exceeded expectations, in terms of value to their area)*	>95%

Avon & Somerset Police and OPCC Proposed Internal Audit Plan 2020/21 APPENDIX 1

It should be noted that the audit titles and high-level scopes included below are only indicative at this stage for planning our resources. At the start of each audit, an initial discussion will be held to agree the specific terms of reference for the piece of work, which includes the objective and scope for the review.

Link to Risk Registers & FMS Area	Areas of Coverage and Brief Rationale	Proposed Days	Proposed Timing
SRR8 - The requirement to improve the Force's overarching Information Governance due to the risks associated with noncompliance against legislation namely the General Data Protection Regulations / Data Protection Act 2018 and associated codes of practice. *(Force Strategic Risk Register Jan 2020)* **FMS Link: IT & Information Management**	**Data Protection – Incident Reporting** *A review assessing the controls in place to report incidents/breaches under the General Data Protection Regulations (GDPR) and compliance with requirements of the legislation. Are the Force and OPCC compliant with reporting and training requirements?*	10	Quarter 1
SRR2 - Combined effects of growing organisation *(Force Strategic Risk Register Jan 2020)* **FMS Link: Force Functions**	**Workforce Plan Follow Up** *A review following on from the Workforce Plan Review conducted in 2019/20. To provide an update on the progress towards implementing the recommendations raised within this piece of work – have recommendations been fully implemented or are they on their way to implementation?*	7	Quarter 1
SR9 - Failure to deliver effective and efficient collaborations or outcomes with other partners" (SR9) *(OPCC Strategic Risk Register Jan 2020)* **FMS Link: OPCC Specific Activity**	**Partnership Arrangements** *A review of the effectiveness of the OPCC's partnership arrangements, in particular Community Safety Partnerships. How are these Partnerships exercising effective governance? Are these partnerships adequately managed in terms of funding and tracking outcomes under the agreements?*	10	Quarter 1
SRR6 - As a critical asset, poor information / quality of data affects decision making across the organisation impacting operationally, tactically and strategically *(Force Strategic Risk Register Jan 2020)* **FMS Link: IT & Information Management**	**Records/Data Retention** *A comparison between controls and requirements, particularly regarding crime archive and helping to improve route to compliance. This piece will look to dovetail with work already completed by the Force and seek to provide assurance that issues identified around data retention within the Personal Issue of Assets review are mitigated against, for example looking to confirm the ability of being able to destroy data remotely. Is the Force complying with requirements under GDPR and any legal requirements around record retention?*	15	Quarter 2
SRR1 - Loss of legitimacy and public confidence *(Force Strategic Risk Register Jan 2020)* **FMS Link: Force Wellbeing**	**Health and Safety Management of Front-Line Staff and Officers** *A review of health and safety arrangements for front-line staff and officers at the Force. How does the Force ensure adherence to applicable laws and regulations around Health and Safety and how effective are the governance and oversight arrangements to protect front-line police officers and staff? How*	15	Quarter 2

	effective are controls and initiatives, such as the seven-point promise (response to assault on officers) and those around staff and officer mental health?		
SRR3 - Lack of capacity and/or capability to deliver an effective policing service *(Force Strategic Risk Register Jan 2020)* **FMS Link: IT & Information Management**	**Digital Strategy** *This review will examine the frameworks and plans (e.g. people, process and technology) in place to realise the delivery of the ambition set out in the Digital Strategy. The scope of this audit will be further refined and agreed with key stakeholders in advance of the fieldwork.*	15	Quarter 3
SRR5 – Failure to effectively plan and manage financial resources *(Force Strategic Risk Register Jan 2020)* **FMS Link: Finance**	**Payments to Staff – Absence Management** *A review of payments made to staff, in particular adherence to the Absence Management Policy. Are payments made to staff in line with the Policy (e.g. sick pay being reduced to half when appropriate) and timescales adhered to?*	10	Quarter 3
SRR5 – Failure to effectively plan and manage financial resources *(Force Strategic Risk Register Jan 2020)* **FMS Link: Finance**	**Key Financial Controls to include Accounts Payable, General Ledger and Aged Debt Management** *Accounts Payable is generally an area of high risk within Finance. This review will focus on the authorisation of payments made, P2P and separation of duties throughout the Accounts Payable Function and will consider the use of robotics/automation in the ordering process. We will also consider the key controls pertaining to the general ledger. For the remaining days, to consider how well the Force is managing its aged debts.*	23	Quarter 3
SRR3 - Lack of capacity and/or capability to deliver an effective policing service *(Force Strategic Risk Register Jan 2020)* **FMS Link: Force Functions**	**Recruitment & Vetting Processes** *E-recruitment system is being implemented at start of the new financial year. A review of this area to include consideration of the new control environment and benefits of transferring from paper-based processes and giving consideration to the use of robotics in this area. Vetting is in preliminary discussions about regional collaboration which is due to be incorporated in a piece of regional work. Is the Force complying with its own and national vetting requirements for both new employees, contractors and renewals for existing employees?*	15	Quarter 4
SRR3 - Lack of capacity and/or capability to deliver an effective policing service *(Force Strategic Risk Register Jan 2020)* **FMS Link: Force Functions**	**Performance Management** *A review of the processes utilised by Supervisors, Sergeants and Inspectors to manage the performance of front-line Police Officers, both individually and on a team basis. How meaningful is the data, such as that derived from Qlik, supporting the Force's aims and objectives around culture and leadership, particularly during the officer uplift? How well does the Force understand the effectiveness of its performance mechanisms across the organisation?*	15	Quarter 4
SRR7 - Failure to deliver sufficient progress towards Police and Crime Plan priorities and ambitions *(Force Strategic Risk Register Jan 2020)*	**Police Officer and Police Staff Training** *A review of the training mechanisms/processes in place for new officers and staff. What subject-specific training has been agreed for new employees to help them in their role and how does this link to*	15	Quarter 4

FMS Link: Force Functions	*workforce planning in terms of the skills that the Force feels it needs? How is this evaluated on an ongoing basis for effectiveness? For officers, how has training been impacted/improved by internal tutoring? Do these tutors have the right skills/experience? How is the relationship with the University of the West of England assisting with development?*		
N/A **FMS Link: Collaborations**	**Contribution to Regional Police Audit Work** *Force contribution to regional working across SWAP Police Partners. Area(s) of coverage determined at regional Directors of Finance meeting, to include vetting and environmental action.*	5	Throughout Year
N/A **FMS Link: Governance, Fraud and Risk Management**	**Follow Up of Partial Assurance Reviews** *Allocation of time to allow for follow up of recommendations resulting from Partial opinion reviews in 2019/20 not subject to separate consideration.*	10	Throughout Year
N/A **FMS Link: Governance, Fraud and Risk Management**	**Planning, Reporting and Advice** *Agreed allocation for attendance at Audit Committees, audit planning and any corporate advice.*	20	Throughout Year
	Total	**180**	

APPENDIX 2

The Internal Audit Charter

Purpose

The purpose of this Charter is to set out the nature, role, responsibility, status and authority of internal auditing within Avon & Somerset Police and Office of the Police and Crime Commissioner (OPCC), and to outline the scope of internal audit work.

Approval

This Charter is presented for approval by the Joint Audit Committee (JAC) on 19 March 2020 and is reviewed each year to confirm it remains accurate and up to date. It was last reviewed by the Joint Audit Committee (JAC) on 10th July 2019.

Provision of Internal Audit Services

The internal audit service is provided by the SWAP Internal Audit Services (SWAP). This charter should be read in conjunction with the Service Agreement, which forms part of the legal agreement between the SWAP partners.

The budget for the provision of the internal audit service is determined by Avon & Somerset Police and Office of the Police and Crime Commissioner (OPCC), in conjunction with the Members Meeting. The general financial provisions are laid down in the legal agreement, including the level of financial contribution by the organisation, and may only be amended by unanimous agreement of the Members Meeting. The budget is based on an audit needs assessment that was carried out when determining the organisation's level of contribution to SWAP. This is reviewed each year by the S151 Officer in consultation with the Chief Executive of SWAP.

Role of Internal Audit

The Accounts and Audit (England) Regulations 2015, state that: *"A relevant authority must undertake an effective internal audit to evaluate the effectiveness of its risk management, control and governance processes, taking into account the public sector internal auditing standards or guidance."*

Internal audit is an independent, objective assurance and consulting activity designed to add value and improve the Organisation's operations. It helps Avon & Somerset Police and Office of the Police and Crime Commissioner (OPCC), accomplish their objectives by bringing a systematic disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.

Responsibilities of Management, Joint Audit Committee (JAC) and Internal Audit

Management[1]

Management is responsible for ensuring SWAP has:

- the support of management and the organisation;
- direct access and freedom to report to senior management, the Section 151 Officer, the Chief Executive of the OPCC and the JAC; and
- Notification of suspected or detected fraud, corruption or impropriety.

Management is responsible for maintaining internal controls, including proper accounting records and other management information suitable for running the Organisation. Management is also responsible for the appropriate and effective management of risk.

JOINT AUDIT COMMITTEE (JAC)[2]

The JAC is responsible for approving the scope of internal audit work, receiving communications from the SWAP Assistant Director on the progress of work undertaken, reviewing the independence, objectivity, performance, professionalism and effectiveness of the Internal Audit function, and obtaining reassurance from the SWAP Assistant Director as to whether there are any limitations on scope or resources.

[1] In this instance Management refers to the Senior Management Team and Statutory Officers.

[2] In this instance Joint Audit Committee (JAC) relates to "The Board" referred to in the PSIAS.

Internal Audit

The SWAP Assistant Director, as Head of Internal Audit, is responsible for determining the scope, except where specified by statute, of internal audit work and for recommending the action to be taken on the outcome of, or findings from, their work.

Internal audit is responsible for operating under the policies established by management in line with best practice.

Internal audit is responsible for conducting its work in accordance with the mandatory elements of the Code of Ethics and Standards for the Professional Practice of Internal Auditing as set by the Institute of Internal Auditors and further guided by interpretation provided by the Public Sector Internal Audit Standards (PSIAS) and the CIPFA Local Government Application Note. SWAP has been independently assessed and found to be in Conformance with the Standards.

Internal audit is not responsible for any of the activities which it audits. SWAP staff will not assume responsibility for the design, installation, operation or control of any procedures. SWAP staff who have previously worked for the organisation will not be asked to review any aspects of their previous department's work until one year has passed since they left that area.

Relationship with the External Auditors/Other Regulatory Bodies

Internal Audit will co-ordinate its work with others wherever this is beneficial to the organisation.

Status of Internal Audit in the Organisation

The Chief Executive of SWAP is responsible to the SWAP Board of Directors and the Members Meeting. Appointment or removal of the Chief Executive of SWAP is the sole responsibility of the Members Meeting.

The Chief Executive for SWAP and Assistant Director also report to the Section 151 Officer, and reports to the Audit Committee as set out below.

The Assistant Director will be the first and primary point of contact for the organisation for all matters relating to the JAC, including the provision of periodic reports, as per company policy. The Assistant Director is also responsible for the design, development and delivery of audit plans, subject to the agreement of Avon & Somerset Police and OPCC.

Scope and authority of Internal Audit work

There are no restrictions placed upon the scope of internal audit's work. SWAP staff engaged on internal audit work are entitled to receive and have access to whatever information or explanations they consider necessary to fulfil their responsibilities to senior management. In this regard, internal audit may have access to any records, personnel or physical property of the organisation.

Internal audit work will normally include, but is not restricted to:

- reviewing the reliability and integrity of financial and operating information used for operational and strategic decision making, and the means used to identify, measure, classify and report such information;
- evaluating and appraising the risks associated with areas under review and make proposals for improving the management and communication of risks;
- appraise the effectiveness and reliability of the enterprise risk management framework and recommend improvements where necessary;
- assist management and Members to identify risks and controls with regard to the objectives of the organisation and its services;
- reviewing the systems established by management to ensure compliance with those policies, plans, procedures, laws and regulations which could have a significant impact on operations and reports, and determining whether the organisation is in compliance;
- reviewing the means of safeguarding assets and, as appropriate, verifying the existence of assets;
- appraising the economy, efficiency and effectiveness with which resources are employed;

- reviewing operations or programmes to ascertain whether results are consistent with established objectives and goals and whether the operations or programmes are being carried out as planned, with performance and accountabilities established.
- reviewing the operations of the organisation in support of their anti-fraud and corruption policy, ethical expectations and corporate values, investigating where necessary.
- at the specific request of management, internal audit may provide consultancy services (including fraud investigation services) provided:
    - the internal auditor's independence is not compromised
    - the internal audit service has the necessary skills to carry out the assignment, or can obtain such skills without undue cost or delay
    - the scope of the consultancy assignment is clearly defined and management have made proper provision for resources the work.
    - management understand that the work being undertaken is not internal audit work.

Planning and Reporting
SWAP will submit to the JAC for approval, an annual internal audit plan, setting out the recommended scope of their work in the period.

The annual plan will be developed with reference to the risks the organisation will be facing in the forthcoming year, whilst providing a balance of current and on-going risks, reviewed on a cyclical basis. The plan will be reviewed on a quarterly basis to ensure it remains adequately resourced, current and addresses new and emerging risks.

SWAP will carry out the work as agreed, report the outcome and findings, and will make recommendations on the action to be taken as a result to the appropriate manager and Chief Finance Officer. SWAP will report at least two times a year to the JAC or as agreed. SWAP will also report a summary of their findings, including any persistent and outstanding issues, to the JAC on a regular basis.

Internal audit reports will normally be by means of a brief presentation to the relevant manager accompanied by a detailed report in writing. The detailed report will be copied to the relevant line management, who will already have been made fully aware of the detail and whose co-operation in preparing the summary report will have been sought. The detailed report will also be copied to the Section 151 Officer and to other relevant line management.

The Assistant Director will submit an annual report to the JAC providing an overall opinion of the status of risk and internal control within Avon & Somerset Police and OPCC, based on the internal audit work conducted during the previous year.

In addition to the reporting lines outlined above, the Chief Executive of SWAP and Assistant Directors have the unreserved right to report directly to the Chair of the Audit Committee, the OPCC's Chief Executive Officer or the External Audit Manager.

A Move to Agile Auditing

When delivering the 2020/21 Internal Audit Programme of work, as presented, we will be looking to embrace the concept of Agile Auditing.

What is Agile Auditing?

Agile Auditing breaks a typical audit engagement down into several shorter stages, with us reporting any findings as we go. It involves increased communication and collaboration with stakeholders throughout the audit process, with greater speed but also transparency. It is likely to involve a team of audit staff instead of one individual.

Why the move to it?

- We recognise that the speed of change (and subsequent risk) is increasing within our Partners. As auditors we therefore need to adapt in order to be able to react and respond quicker.
- We constantly seek ways in which we can add value to our Partners, in order to help them succeed. Increased communication and collaboration through Agile Auditing will support this.
- We also want to move towards shorter and more impactful audit reports; Agile Auditing will facilitate this.

What will it involve?

As above, an Agile audit engagement is likely to involve a small team of audit staff as opposed to one individual. This will ensure that the audit proceeds and concludes with greater pace.

Although we are likely to require more frequent interaction with staff in the area we are auditing, the interaction will be quicker and more focussed. We are confident that the overall time required from staff will actually be less than through a traditional audit approach.

We will look to discuss any audit findings with staff throughout the stages of the audit. This will ensure that by the time we come to report, we already have agreement to any proposed actions required, and even provide the opportunity for any findings to be actioned prior to the completion of our audit.

What will be the benefits?

- ☑ **Ability to provide faster assurance**
- ☑ **Enhanced ability to add value**
- ☑ **Audit observations resolved more quickly**
- ☑ **Shorter, more impactful audit reports**
- ☑ **Reduced negotiations at audit report start**

We hope you support our move towards Agile Auditing.

If you would like to discuss the concept in more detail, please speak to your SWAP contact.

AVON & SOMERSET
POLICE & CRIME
COMMISSIONER

SWAP
INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

6b

Avon & Somerset Constabulary

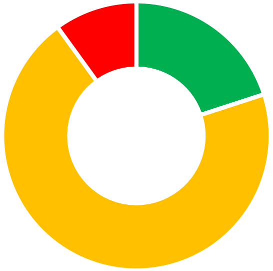
Cyber Security

Final Report

Issue Date: 10 March 2020

Executive Summary

Audit Summary



This review has been undertaken against 20 agreed Key Cyber Security controls.

We would suggest that management give attention to the recommendations for immediate action within this report.

Consideration should also be given to the areas highlighted for potential future audit review.

Opinion	Number
Fully compliant	4
Recommended further review	14
Requires immediate attention	2
Total	**20**

Audit Conclusion

The 20 Key Cyber Security Controls have each been given an initial assessment on page 3 below. The findings of this report should be used by management to address areas that require immediate attention and as a catalyst for discussion during the annual audit planning process with a view to future audit work.

Significantly, there have been two recent assessments completed in relation to the Constabulary's maturity for information and cyber security:

1. The National Institute of Standards and Technology (NIST) Cyber Security Framework as part of the National Enabling Programme (NEP) Security Model was assessed in July 2019. 19 key controls were identified by the National SIRO and a risk statement for these has been completed together with a timescale for completion, the action required and a responsible officer. During the audit we found that two of the agreed actions had passed the implementation date without progress. The remaining 76 have been pulled into a local remedial plan however, but have no timescale or responsibility attached and have not been considered for prioritisation.

2. An IT Health-check security assessment was conducted independently in October 2019 and a total of 124 vulnerabilities noted in the conclusion, of which 3 are critical and 20 are classified as high. There is no remediation plan in relation to these vulnerabilities.

Recommendations have been raised regarding the above, however the Director of IT felt that the actions required under the recommendations were already in progress as a result of the recent NIST (NEP) and IT Health-check assessments. The recommendations have been included for information, together with the context from the Director of IT, however it must be noted that SWAP has not reviewed evidence to support the comments made.

There are four additional recommendations made, where it was deemed that immediate action should be undertaken by management to reduce risk exposure. These are summarised as follows:

Governance of Information Security

The Information Security Manual, which acts as the framework and directive for information security is currently under review. There are opportunities to strengthen the control framework prior to the publication of the revised document, which are noted in 1.1 of the main report below.

These ideas include the attachment and reference to a set of sub policies and the introduction of compliance software which will ensure all staff are obliged to read and understand key documents.

Key Vacancy

The Information Security Officer post has been vacant for 14 months. This role is being covered by an officer with conflicting priorities. It is acknowledged that there is a national difficulty in recruiting for this position, but the importance of the position is directly linked to the number of recommendations made in both this review and the two previous assessments on security referenced above.

Technical Security Strategy

Although there is a requirement for compliance with the National Enabling Programme, there is currently no technical security strategy for the Force. The introduction of a local strategy would enable better understanding of direction and what dependencies are needed to move forward.

Vulnerability Testing

We did not have sight of an agreed and established programme of work in relation to penetration testing. The Constabulary should be considering the threat landscape for cyber and assigning vulnerability testing in line with an agreed risk tolerance level. The Director of IT confirmed (as per Section 1.5 below) the scenarios which would require penetration testing and that this is covered annually by the IT Health Check. As above, the details are included for management information.

Audit Scope

In order to mitigate against threats that could prevent the business continuity of ICT services and/or the loss or corruption of data, the Constabulary needs to manage controls to maintain healthy cyber security across the ICT enterprise. Cyber threats could come from malicious activity either inside the perimeter or from external sources, user error or incidents outside of the organisations control such as power failures or the loss of a communications network.

By undertaking an analysis of cyber security matched with an agreed risk assessment, the Constabulary can make arrangements to mitigate these threats using specific tools, policies and processes. If controls surrounding cyber security are not managed, then the organisation will remain exposed to a potential loss of ICT Business Continuity which could result in a wider organisational Business Continuity incident. There will also remain the risk that data could be lost, corrupt or stolen which will have an impact on the organisation regarding their compliance with the revised requirements of the General Data Protection Regulation (GDPR) introduced in May 2018.

A total of 20 key cyber security controls were programmed for review in this audit. There is a significant overlap between the agreed SWAP work template and the testing completed in the recent NIST (NEP) and IT Health-check assessments. In order to avoid unnecessary duplication, it was agreed that we would, where possible, place reliance on the work completed elsewhere.

Findings and Outcomes

Summary of Control Framework

One added value element to this review is that it will allow the Force to benchmark its results against other SWAP partners, including police forces, to identify areas of best practice and potentially where resources and controls relating to cyber security could be shared.

We have provided outcomes for each of the 20 key controls below:

Key Control Area:	Fully compliant	Recommended for further review	Requires immediate attention
Cyber Security Governance and Management Support			🟥
Existence and Maintenance of an Inventory of Hardware Assets		🟨	
Inventory of Software Assets (including Data Assets)		🟨	
Vulnerability Management Processes		🟨	
Control of Accounts with Administrative Privileges		🟨	
Deployment of Secure Hardware and Software Configurations	🟩		
Active Monitoring and Analysis of Audit Logs		🟨	
E-Mail and Web Browser Protections	🟩		
Deployment of Malware Defences		🟨	
Control of Network Ports, Protocols and Services		🟨	
Data Recovery Capabilities including Back Up and Restore		🟨	
Secure Configuration of Network Devices		🟨	
Boundary Defences are documented and understood	🟩		
Management controls for data in transit		🟨	
Management of Wireless Access Controls		🟨	
User Access Monitoring and Control		🟨	
Security Awareness and Training		🟨	
Development of Application Software and Security	🟩		
Incident Response and Management Procedures		🟨	
Programme of Penetration Testing			🟥

Areas Requiring Immediate Attention from Management

1.1	Finding and Action

Key Control Area and Issue	Risk
Cyber Security Governance and Management Support – The Information Security Manual requires approval.	Key stakeholders are not given accurate information regarding information security, leading to inconsistencies in application and possible breach, resulting in financial loss, reputational damage and/ or loss of service.

Findings

The Information Security Manual acts as the overarching framework and directive for information security. This document is owned by the SIRO and is based on the ISO 27001 (ISMS) model and the Secure Policy Framework: protecting government assets. The manual is under review by the acting Information Security Officer, so the old version is currently available to staff through Pocket Book. The main changes to the revised manual are in relation to personnel, governance and there are references to policies that have been removed or superseded.

There are several other policies that have an information security focus, including the Internet System Security Manual, IT Acceptable Usage and the procedural guidance for Cyber Incident Response. The Constabulary should consider the framework for information security with a view to linking these other polices to the Information Security Manual. This would allow for better governance and maintenance of change control over the whole framework.

Finally, there is no mechanism for ensuring that staff and volunteers have read and understood the key policies relating to Information Security.

Recommendation

We recommend that the Senior Information Risk Owner ensures that the Information Security Manual is approved by the Strategic Information Management Board. The updated manual should then be made known and available to all staff.

Consideration should be given to implementing controls that would see staff confirm that they have read and understood the key policies in relation to information security. Use of compliance software or changes to the induction process would be examples of how this can be enforced.

Prior to publishing this document, the SIRO should consider the wider links to other policy areas with a view publishing them as a subset of policies to the Information Security Manual.

Agreed Action	Timescale	31/05/2020
The latest draft of the Information Security manual will be reviewed against other related policies and presented at the May Strategic Information Management Board for formal SIRO approval. Note: A compliance tool is currently being tested for deployment later this year This will be used to monitor staff readership and acceptance of policies.	Responsible Officer	Director of Information Technology

<table>
<tr><th>1.2</th><th colspan="4">Finding and Action</th></tr>
<tr><td colspan="3">Key Control Area and Issue</td><td colspan="2">Risk</td></tr>
<tr><td colspan="3">Cyber Security Governance and Management Support – The Information Security Officer post is vacant.</td><td colspan="2">The key vacancy increases the risk of service disruption, financial loss and reputational damage.</td></tr>
<tr><td colspan="5">Findings</td></tr>
<tr><td colspan="5">The information Security Officer post has been vacant for around 14 months and is being covered by the IT Service Manager. A job role profile has been drafted for this position and it is noted that has been a difficulty in recruiting for this role nationally. Two deadlines have recently been missed in relation to recommendations following the NIST assessment. Missed deadlines could result in delays to the technical pilot and failure to meet NEP objectives. A dedicated resource for information security would reduce this risk.</td></tr>
<tr><td colspan="5">Recommendation</td></tr>
<tr><td colspan="5">We recommend that the SIRO in liaison with the Strategic Information Management Board reviews and approves the job role documentation for the Information Security Officer (ISO) post. An adequate handover period from the acting ISO should also be scheduled.</td></tr>
<tr><td colspan="3">Agreed Action</td><td>Timescale</td><td>31/05/2020</td></tr>
<tr><td colspan="3">The current draft role profile for the ISO role will be completed and regraded once decisions are made on the placement of the role within the ASC enabling services. Preparatory work for this activity will complete during March and April. This will be presented for SIRO approval.</td><td>Responsible Officer</td><td>Director of Information Technology</td></tr>
</table>

<table>
<tr><th>1.3</th><th>Finding and Action</th></tr>
<tr><td>Key Control Area and Issue</td><td>Risk</td></tr>
<tr><td>Cyber Security Governance and Management Support – There is no technical security strategy.</td><td>The Constabulary will not be able to demonstrate the effectiveness of its service provision in relation to information security. This could lead to non-compliance with the GDPR and result in significant financial loss and reputational damage.</td></tr>
<tr><td colspan="2">Findings</td></tr>
<tr><td colspan="2">It is best practice to have an effective technical security strategy which should align with dependant strategies and with legal and regulatory requirements. It will outline the mitigations to manage risks to an acceptable level, using security resources effectively. It should provide the channel to get engagement from management and staff to communicate the information security requirements in line with the stated objectives.
Although there is a requirement for compliance with the National Enabling Programme, there is currently no technical security strategy for the Constabulary.</td></tr>
<tr><td colspan="2">Recommendation</td></tr>
<tr><td colspan="2">We recommend that the IT Director considers the creation of a Force specific IT security strategy which sets out deliverables, capacity, associated costs, key dependencies, responsibilities and priorities for IT security. This should be:
▪ Considered in line with appointment of an Information Security Officer</td></tr>
</table>

▪ Drafted through discussion with other key stakeholders including the SIRO ▪ Completed with consideration to the NEP ▪ Approved by the Strategic Information Management Board		
Agreed Action	Timescale	31/12/2020
Document a Force specific IT security strategy which sets out deliverables, capacity, associated costs, key dependencies, responsibilities and priorities for IT security. This should be: ▪ Considered in line with appointment of an Information Security Officer ▪ Drafted through discussion with other key stakeholders including the SIRO ▪ Completed with consideration to the NEP and other Regional and National Systems ▪ Approved by the Strategic Information Management Board	Responsible Officer	Director of Information Technology

1.4 Finding and Action	
Key Control Area and Issue	Risk
Cyber Security Governance and Management Support – There are no timescales and responsibilities assigned to the NIST assessment actions.	Without a plan to manage the implementation of highlighted weaknesses there is increased risk of service disruption, financial loss and reputational damage.
Findings	
The recent (Oct 2019) Security Model (NIST) assessment completed by Deloitte reviewed a list of 183 controls relating in line with the National Enabling Programme. There are 95 control weaknesses identified in total. 19 key controls were identified by the National SIRO and a risk statement for these has been completed together with a timescale for completion, the action required and a responsible officer. The remaining 76 have been pulled into a local remedial plan however, but have no timescale or responsibility attached and have not been considered for priority.	
Recommendation	
We recommend that the IT Director, in liaison with the NEP Project Manager considers timescales and assignment of responsibility for the remedial actions following the control weaknesses identified in the NEP security model assessment. A risk-based view on this is recommended and a mechanism for monitoring the progress and implementation of each weakness should also be established.	
Comments from the Director of Information Technology	
This action inevitably follows the assessment and is driven through the NEP programme. The NIST results get incorporated into the Security Model and we get a compliance figure on it. In the initial round of checks we were at 67% compliant. Following the latest round of checks we are now at 82% compliance. Due to the remediation often covering more than one control, it is easier to quote %'s rather than responding to individual controls. The remediation plan covers the requirements rather than fixing singular controls.	

1.5 Finding and Action

Key Control Area and Issue	Risk
Programme of Penetration Testing – There is no agreed programme for penetration testing and there are no timescales and responsibilities assigned to the vulnerabilities identified in the most recent review.	Without a plan to identify and manage external vulnerabilities there is increased risk of service disruption, financial loss and reputational damage.

Findings

There is no established programme of work in relation to penetration testing. The November 2019 NIST assessment found that around 50% of the NEP build had been pen tested. The remaining 50% is programmed for testing in early 2020.

An ICT Health-check report was completed in October 2019 and this included an external infrastructure and multiple firewall assessments.

There are 124 vulnerabilities noted in the conclusion of the most recent IT Health-check Security Assessment. Three of which are noted as critical (requires resolution as quickly as possible) and 20 are classified as high (requiring resolution in the short term). There is not yet a remediation plan in place to address the identified weaknesses.

Recommendation

We recommend that the IT Director documents a schedule for the ongoing testing of vulnerabilities in line with a risk appetite which is accepted and agreed by the Information Security Review Group.

Comments from the Director of Information Technology

Pen tests are routinely commissioned when new capabilities are introduced, or risks are identified. We also have a requirement to commission an IT Health check annually. We consider the scope of that during the summer and procure and execute it in the Autumn. The Information Security Group monitors this.

Recommendation

We recommend that the IT Director implements a remediation plan in relation to the IT Health-check security assessment. This should include the assignment of responsibility for the remedial actions and an agreed timescale for completion. A risk-based view on this is recommended and a mechanism for monitoring the progress and implementation of each weakness should also be established.

Comments from the Director of Information Technology

A remediation plan always follows an IT Health-check security assessment. This has been completed and also shared with the national accreditor and NEP programme. Actions are allocated to teams and monitored weekly/bi-weekly.

Authors and Distribution

Please note that this report has been prepared and distributed in accordance with the agreed Audit Charter and procedures. The report has been prepared for the sole use of the Partnership. No responsibility is assumed by us to any other person or organisation.

Report Authors

This report was produced and issued by:

Dave Warren	Senior Auditor, SWAP Internal Audit Services
Darren Roberts	Assistant Director for IT, SWAP Internal Audit Services
Laura Wicks	Assistant Director for Emergency Services, SWAP Internal Audit Services

Distribution List

This report has been distributed to the following individuals:

Nick Lilley	Director of Information Technology
Sarah Crew	SIRO and Deputy Chief Constable
Jane Walmsley	Inspection and Audit Coordinator
Nick Adams	Chief Officer – Finance, Resources and Innovation

AVON & SOMERSET
POLICE & CRIME
COMMISSIONER

SWAP
INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

6c

Avon and Somerset Police

IT Business Continuity

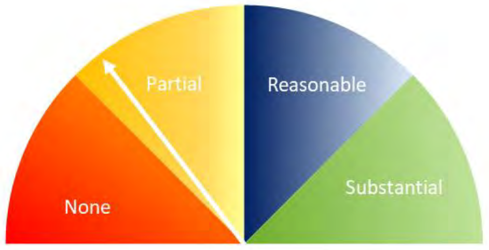
Final Report

Issue Date: 10 March 2020

Working in Partnership to Deliver Audit Excellence

Executive Summary

Audit Opinion



Partial

In relation to the areas reviewed and the controls found to be in place, some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.

Recommendation Summary

Priority	Number
Priority 1	**0**
Priority 2	**4**
Priority 3	**0**
Total	**4**

Audit Conclusion

Effectiveness of Control Framework

- Our review has highlighted some significant gaps in the framework of documentation in place at the Constabulary to ensure business continuity in the event of an incident that disrupts operations. The development of this framework of documentation has been hindered by other contingency planning priorities such as Brexit. As a result of the limited documentation in place surrounding business continuity planning, the assurance opinion we have been able to able to provide in with area is Partial.
- The assurance opinion we have been able to provide does not reflect on the ability of decision makers to respond to an incident but is based on the formally documented business continuity planning procedures and policies in place we were able to review.

Design of Control Framework

A number of weaknesses were identified in the Design of the Control Framework in relation to IT Business Continuity, which has considerably impacted our assurance opinion. Whilst the Constabulary's Contingency Planning and Business Continuity Department is responsible for co-ordinating business continuity planning across the organisation there were a number of areas where findings were identified:

- A strategic level Crisis Management Plan is in place which focuses on how to manage issues at a strategic level. This plan should be invoked during incidences which threaten the Constabulary's ability to deliver business critical services on a force-wide level. Examples include pandemic disease, industrial action and a loss of key premise such as the Police Headquarters.
- An action plan has been developed by the Contingency Planning and Business Continuity Department in January 2020 to help ensure that a BCP is in place for all services. However, we are concerned that this action plan may not be adequately supported or monitored by Senior Management to ensure goals and objectives are met in a timely manner.
- Business Continuity Plans (BCP), which outline how to deal with and manage incidences at a tactical and operational level, are not in place for the majority of services or remain in the process of being drafted.

- Business critical IT systems and operations and their recovery time objectives (RTOs) have yet to be fully defined by the Constabulary. Business critical IT systems and operations are those that are essential to ensure a continuity of business operations. These currently include the Constabulary's police records management system (NICHE); its finance, payroll and HR system (SAP) and its command and control system (STORM). RTOs are the targeted duration of time and service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity.
- Where business critical IT systems, operations and RTOs have not been defined, in the event of a loss of IT availability, there is a risk that the IT Service may not be able to achieve recovery of IT systems that are critical to business continuity due to demand / inadvertent focus on recovery of non-critical systems. This could result in financial loss, reputational damage, legal challenge and the safety of the public being compromised.

Application of Control Framework

- To date, six out of 26 services have a BCP in place. A further two service level BCPs are in draft. A progress summary of service level BCPs has been provided within Appendix A. Without service level BCPs in place, there is a risk that the Constabulary may not be adequately prepared to respond to the impact of an incident affecting one or more of its services. This could lead to inability to deliver an ongoing service which may result in financial loss, reputational damage, legal challenge and the safety of the public being compromised.
- The Contingency Planning and Business Continuity Officer has also raised concerns around the lack of "buy-in" from services surrounding business continuity planning which may adversely impact on BCPs being developed to a satisfactory standard and/or in a timely manner.

Audit Assessment of Agreed Themes

Theme	RAG Rating	Reason for RAG Rating
Leadership & Culture	🟧	The RAG rating we have been able to provide in this area directly correlates to the identified gaps in the framework of documentation in place at the Constabulary to ensure business continuity in the event of an incident that disrupts its operations. The limited progress in developing this framework highlights potential concerns with regards to the leadership, culture and learning surrounding this activity of work.
Learning	🟧	In July 2018, the ownership of the IT Service transferred back from Southwest One to the Constabulary. This included the transfer of all processes, assets and staff back in-house. These arrangements are therefore still in their infancy. This together with the findings highlight within the 'Leadership & Culture' section above has impacted on the RAG rating we have been able to offer.
Diversity and Inclusion	Not Assessed	We have been unable to provide an opinion on diversity and inclusion specific to the processes reviewed.

Background

The Civil Contingencies Act 2004 imposes a statutory duty on Police Forces to undertake business continuity management to prepare, maintain and exercise Business Continuity Plans and the Strategic Policing Requirement places specific business continuity requirements on the Constabulary. Many services within the Constabulary are reliant on the provision of IT including applications, communications and infrastructure as part of their operational business continuity. However when the IT provision is not available due to a service disruption, service level business continuity plans need to reflect the criticality of their IT provision and record mitigations that could be in place to maintain a degree of business continuity while IT services are restored. Therefore, a review of business continuity planning arrangements in the event of a critical IT incident has been undertaken.

Corporate Risk Assessment

Audit Objective

To ensure that the organisation has planned for and can maintain an agreed level of business continuity to priority services in the event of a critical IT incident.

Risks	Inherent Risk Assessment	Manager's Initial Assessment	Auditor's Assessment
Over reliance on the IT service to maintain Corporate business continuity resulting in a loss of organisation wide service continuity in the event of a disruption to IT services.	**High**	**High**	**High**

Scope

The audit considered the following:

- Whether critical IT services and operations within service level Business Continuity Plans (BCP) have been identified.
- The expectations of the IT Service regarding resource and capacity to enable availability of key applications, infrastructure, communications and platforms following an incident that disrupts the Constabulary's operations.
- Whether arrangements are in place to allow services to continue to operate following the loss of IT systems or an outage.

Due to the limited framework of documentation in place for business continuity planning, we were unable to do consider the following areas which had originally been included within the intended scope:

- The processes in place to review and update BCPs including where BCPs have been invoked and a lesson learnt exercise have been undertaken.
- The framework for periodically testing BCPs plans in place to ensure that they are adequately resourced.

Recommendations have been raised to address these areas as outlined in Section 1.2 below.

Findings and Outcomes

1. Over reliance on the IT service to maintain Corporate Business Continuity resulting in a loss of organisation wide service continuity in the event of a disruption to IT services.	High

1.1	Finding and Action

Issue	Risk
Business critical IT systems and operations and their recovery time objectives (RTO) have not yet been fully identified and agreed.	In the event of a loss of IT availability, the IT Service may not be able to achieve recovery of IT systems that are critical to business continuity due to demand / inadvertent focus on recovery of non-critical systems. This could result in financial loss, reputational damage, legal challenge and the safety of the public being compromised.

Findings

Business critical IT systems and operations are those that are essential to ensure business continuity. A recovery time objective (RTO) is the targeted duration of time and a service level within which a business process must be restored after a disaster or disruption in order to avoid unacceptable consequences associated with a break in business continuity. Both business critical systems and RTOs have not yet been fully defined by the Constabulary.

The IT Service is currently in the process of producing an initial list of business-critical systems (known as CAT A systems). Business critical systems currently include (but are not limited to) the Constabulary's police records management system (NICHE); its finance, payroll and HR system (SAP) and its command and control system (STORM). Once these critical systems have been documented, all services will be required to confirm that these are in fact critical systems to business continuity and set appropriate RTOs. The achievability of RTOs will need to be confirmed by IT to ensure that they are appropriate to the resources available. Where systems cannot be restored in line with RTOs, the Constabulary must put in place measures to ensure services can continue to be provided in the event of sustained loss of business-critical IT systems. In addition, some business-critical systems will be dependent on the recovery of a third party. For example, the Police National Computer (PNC) which is used to facilitate investigations and sharing of information. The Constabulary will also need to put in place adequate measures to mitigate against the loss of these third-party systems.

1.1a	Recommendation	
We recommend that the Director of Information Technology, together with all relevant Heads of Service, identifies and agrees a list of all business-critical IT systems and operations and their appropriate recovery time objectives to restore these. Recovery time objectives will need to be confirmed by IT to ensure that they are appropriate to the resources available. This work should also include a review of business-critical systems and operations that are dependent on external providers to recover.	Priority Score	2

Agreed Action	Timescale	30/09/2020
A list of agreed business critical systems was produced in late 2017 with the intention that the list would be owned and maintained by the IT Directorate. This identified 30 'Category A' systems. In 2019, IT began reviewing the disaster recovery arrangements of each system and identified a need to sub categorise them into risk to life; operationally important; and important. This work needs completing with additional RTO objectives agreed and understood by critical business areas. We will complete the review of critical systems and categorisation with all functional owners and ensure that RTO objectives are understood and matched to available skills, resources and third-party contracts.	Responsible Officer	Director of Information Technology

1.2	Finding and Action

Issue	Risk
A service level Business Continuity Plan (BCP) is not in place for all Services.	The Constabulary may not be prepared to adequately respond to the impact of an incident affecting one or more of its services. This could lead to inability to deliver an ongoing service which may result in financial loss, reputational damage, legal challenge and the safety of the public being compromised.

Findings
An up to date business continuity plan (BCP) is in place for six out of the 26 services across the Constabulary (see summary of progress within Appendix A). With regards to the six BCPs already in place, these may need to be revised given the findings detailed within 1.1 above which highlights that business-critical systems and RTOs have not yet been identified and agreed. Therefore, business continuity arrangements to mitigate against the sustained loss of critical IT systems beyond RTOs in order to provide an ongoing service will not have been properly considered as part of the six BCPs in place. The Constabulary's Contingency Planning and Business Continuity Department is responsible for co-ordinating this work. An action plan has been developed by the Contingency Planning and Business Continuity Officer in January 2020 to help ensure that a BCP is in place for all services. In addition, a standard BCP template has been developed to help ensure adequate and appropriate information is captured and service BCPs are consistent across the Constabulary. However, we are concerned that this action plan may not be adequately supported or monitored by Senior Management to ensure goals and objectives are met in a timely manner. The Contingency Planning and Business Continuity Officer has also raised concerns around the lack of buy-in from services surrounding business continuity planning which may adversely impact on BCPs being developed to a satisfactory standard and/or in a timely manner.

1.2a	Recommendation

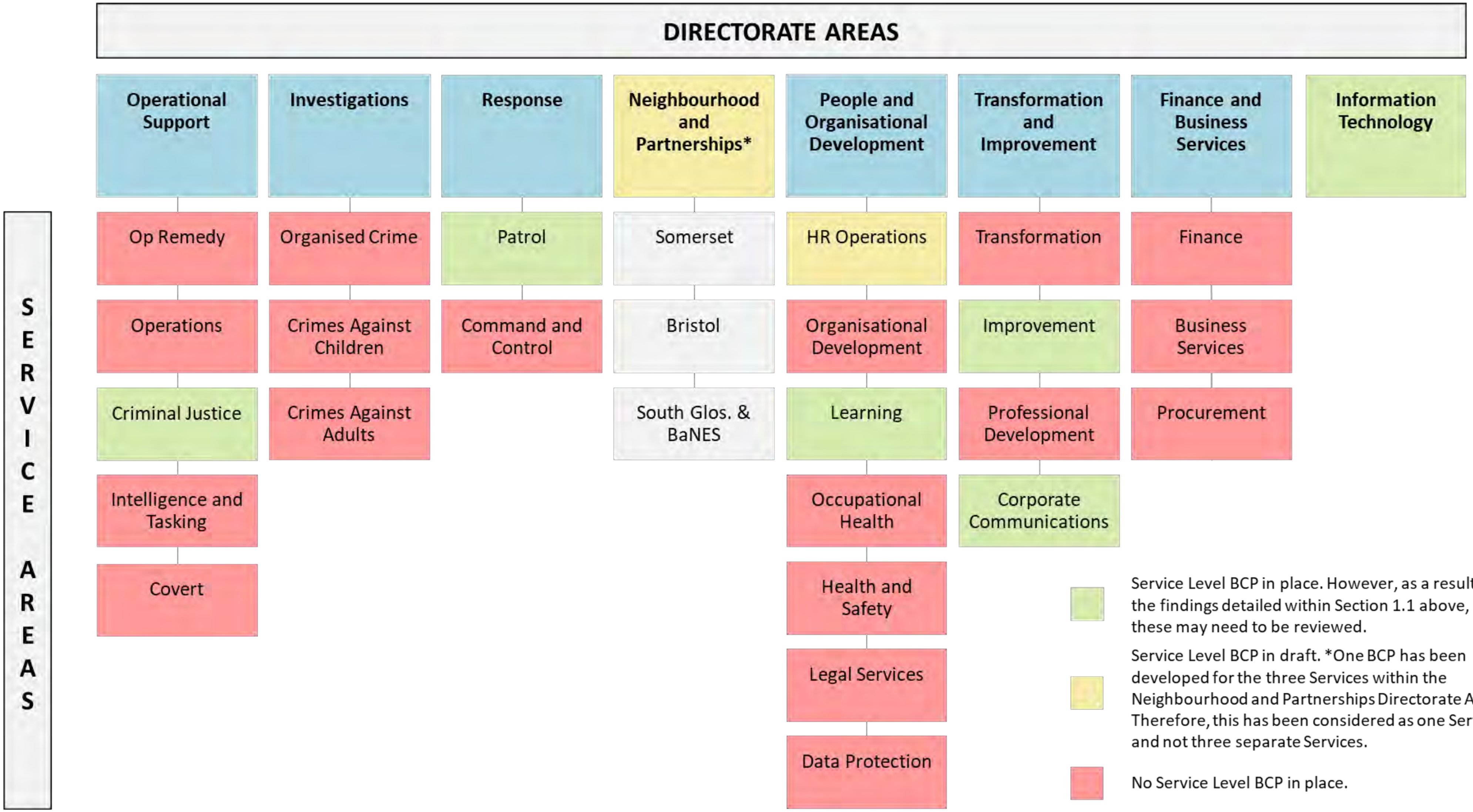
We recommend that the Head of Operational Support, together with all other relevant Heads of Service ensures that service level business continuity plan is in place for all required services across the Constabulary. Service level business continuity plans should:	Priority Score	2

▪ Contain all required information to adequately inform decision making in the event of an incident that causes disruption to business operations. ▪ Be completed consistently with the agreed template. ▪ Have an appropriate review and approval schedule in place including in situations where the service BCP has been invoked. Any lessons learnt carried out following the activation of a BCP should then inform a subsequent review of the BCP. ▪ Be shared and stored across the organisation appropriately in both electronic and hardcopy formats. ▪ Include adequate provisions for business-critical systems that cannot be restored by the IT service within the required timescale for the service. For example, the provisions that will allow HR, Payroll and Finance to continue to operate in the event of a SAP outage. ▪ Have a framework for the testing in place to ensure that BCPs are fully resourced.		
Agreed Action	Timescale	30/09/2020
Collating of the Force Business Continuity Plans (BCPs) is moving at quite a pace now. We have added three specific Estate plans and two departmental ones. We have final meetings booked with business leads, following which the BCPs will be sent to us around mid-March. Our action is to chase up business leads for their BCPs and have all outstanding plans published by the end of April. Storage of the BCPs is on the G:Drive and can be accessed by Units / Department Head / Directorate Head and the Contingency Planning Team. The Framework for checking and testing plans is currently under development.	Responsible Officer	Contingency Planning Officer

1.2b	Recommendation		
We recommend that the Head of Operational Support implements a mechanism to monitor performance of the action plan developed by the Contingency Planning and Business Continuity Department to ensure service level business continuity plans are developed to a satisfactory standard, reviewed and approved in a timely manner. Performance should be reported at a corporate level (e.g. The Constabulary Management Board) to help ensure buy-in and the achievement of goals and objectives.		Priority Score	2

Agreed Action	Timescale	30/09/2020
Plans are prepared by the business lead for the area being considered. Following this, they are signed off by the Head of the Department prior to being signed off by the Directorate Head, who will in turn share this with their COG lead. These will be reviewed on a 6 monthly basis and will eventually be tied in with the framework for checking and testing plans. A Silver Command Group has been formed to manage COVID-19. This will inform key functions of BCP in order to prioritise departments.	Responsible Officer	Contingency Planning Officer
1.2c Recommendation		
We recommend that the Head of Operational Support undertakes a review of all existing service level business continuity plans in place once business critical systems and recovery time objectives have been identified. The review should ensure that existing plans include arrangements to mitigate against the sustained loss of critical IT systems beyond agreed recovery time objectives.	Priority Score	**2**
Agreed Action	Timescale	30/09/2020
The Head of Operational Support will undertake a review of all existing Service Level BCPs (recommendation 1.2a), this will be managed using Trello cards that have been developed to show progress of reviews with new annual review dates which will take into account the above.	Responsible Officer	Head of Operational Support / Contingency Planning Officer

Appendix A: Progress of Service Level Business Continuity Plans



DIRECTORATE AREAS

SERVICE AREAS

🟦 **Operational Support**	🟦 **Investigations**	🟦 **Response**	🟨 **Neighbourhood and Partnerships***	🟦 **People and Organisational Development**	🟦 **Transformation and Improvement**	🟦 **Finance and Business Services**	🟩 **Information Technology**
🟥 Op Remedy	🟥 Organised Crime	🟩 Patrol	⬜ Somerset	🟨 HR Operations	🟥 Transformation	🟥 Finance	
🟥 Operations	🟥 Crimes Against Children	🟥 Command and Control	⬜ Bristol	🟥 Organisational Development	🟩 Improvement	🟥 Business Services	
🟩 Criminal Justice	🟥 Crimes Against Adults		⬜ South Glos. & BaNES	🟩 Learning	🟥 Professional Development	🟥 Procurement	
🟥 Intelligence and Tasking				🟥 Occupational Health	🟩 Corporate Communications		
🟥 Covert				🟥 Health and Safety			
				🟥 Legal Services			
				🟥 Data Protection			

🟩 Service Level BCP in place. However, as a result of the findings detailed within Section 1.1 above, these may need to be reviewed.

🟨 Service Level BCP in draft. *One BCP has been developed for the three Services within the Neighbourhood and Partnerships Directorate Area. Therefore, this has been considered as one Service and not three separate Services.

🟥 No Service Level BCP in place.

Authors and Distribution

Please note that this report has been prepared and distributed in accordance with the agreed Audit Charter and procedures. The report has been prepared for the sole use of the Partnership. No responsibility is assumed by us to any other person or organisation.

Report Authors

This report was produced and issued by:

Laura Wicks	Assistant Director – Emergency Services
Darren Roberts	Assistant Director – IT
Juber Rahman	Senior Auditor

Distribution List

This report has been distributed to the following individuals:

Nick Lilley	Director of Information Technology
Peter Warren	Head of Operational Support
Claire Southwell	Contingency Planning and Business Support Manager
Mark Rose	Contingency Planning Officer
Mark Simmons	Interim Chief Executive Officer
Nick Adams	Chief Finance Officer, Avon and Somerset Constabulary and OPCC
Jane Walmsley	Inspection and Audit Co-Ordinator

AVON & SOMERSET
POLICE & CRIME
COMMISSIONER

SWAP
INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

6d

Avon and Somerset Police

Fleet Management

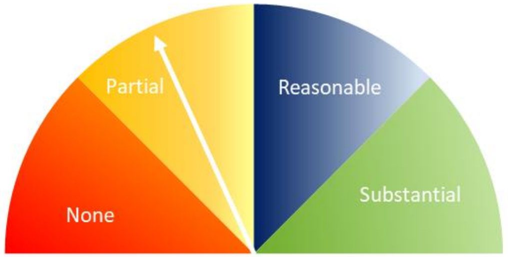
Final Report

Issue Date: 10 March 2020

Working in Partnership to Deliver Audit Excellence

Executive Summary

Audit Opinion



Partial

In relation to the areas reviewed and the controls found to be in place, some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.

Recommendation Summary

Priority	Number
Priority 1	**0**
Priority 2	**5**
Priority 3	**3**
Total	**8**

Audit Conclusion

Effectiveness of Control Framework

- Key performance indicators (KPIs) have been in place since June 2019 and report on the Constabulary's fleet availability and downtime, with an ideal availability level of 95%. The Constabulary's average availability between June 2019 – December 2019 was around 90%, equating to around 120 vehicles off the road. The summer months of June, July and August saw the Constabulary's best fleet availability performance with the highest recorded availability at 92%, likely driven by a higher level of staff overtime undertaken in this period. The average vehicle downtime over the same period is around 18 days. Although not captured within our testing, the availability figures from January and February 2020 demonstrate a more favourable outturn for the service. However, our review has raised concerns over the accuracy of this information as detailed below. Further work is required to improve data quality before these KPIs can provide an accurate reflection of performance and help inform decision making.
- Transport Services have implemented or are in the process of implementing a number of controls and processes to help improve the overall effectiveness of its operations.
- However, a 'Partial' assurance opinion has been provided due to weaknesses identified in the design and application of the current control framework as set out below. Transport Services already recognise some of the weaknesses we have identified in our review and have set objectives under the Infrastructure Strategy (discussed in the 'Background' section below) to help address these. These include improvements to staff training, processes to enhance data quality and the introduction further KPIs to better manage and monitor performance. The findings in this report together with the recommendations raised should help inform solutions implemented by management to address identified weaknesses.

Design of Control Framework

As above, Transport Services have implemented or are in the process of implementing the following controls and processes to help improve the overall effectiveness of its operations:

- Various initiatives to help tackle environmental challenges including the reduction of the fleet by 17 vehicles to introduce more than 70 pedal and electric cycles to help the Constabulary's Neighbourhood Policing Teams move around their areas.
- New telematics systems have been installed in over 220 pool and marked vehicles to enhance reporting capabilities and more effective management of assets. Transport Services are planning to install these systems into over 400 more of their vehicles.
- A number of upgrades are due to be implemented later this quarter to the current Fleet Management System (Tranman). This aims to introduce efficiencies in day to day processes and provides a clearer self-service facility to the organisation.
- Transport Services have been recruiting for eight vacancies which has impacted on their ability to deliver its service. It is estimated that these vacancies will be filled by late Spring 2020.
- The addition of two more local workshops in the Bridgwater and Radstock areas will help deliver both financial and operational efficiencies as well as increase fleet availability.
- The development of technological solutions (referred to as a 'Digital Worker') to schedule jobs and automatically populate information into Tranman.

However, the following weaknesses with the overall design of the control framework were identified:

- Services or 'MOTs' can easily be delayed or missed. ***Under the Motor Vehicles (Tests) Regulations 1981, the Constabulary is exempt from undertaking MOTs but must maintain their vehicles to a high standard in workshops approved by the Secretary of State. All fleet vehicles will therefore undergo an 'MOT' equivalent test each year. (Where reference is made to MOT, this is the equivalent test performed by the Constabulary and not a legal requirement.)*** Where a service or MOT is flagged as required by the Fleet Management System (Tranman), the Admin Hub will raise a job and notify the vehicle owner by email that their vehicle is due a service or MOT. As this process is currently a manual one, there is a risk of human error in not sending out the emails/sending them late. Once the email is sent, it becomes the responsibility of the vehicle owner to schedule and bring in the service or MOT, thus placing the onus on vehicle owners to remember to schedule the job. Going forward, this issue is likely to be resolved by the 'Digital Worker' described above.
- Once a job is raised by the Admin Hub, the system will assume that those vehicles with raised jobs have already been scheduled and these are excluded from future reports unless the job is removed manually. The Admin Hub will usually monitor these scheduling reports to ensure a vehicle has been booked in for work. However, monitoring has been affected by structural changes to the admin service incurred in autumn 2019. As result, some members of staff are new to the organisation / service and still learning processes. Therefore, vehicles which miss their next service or MOT date may not be detected.
- Key performance indicators (KPIs) are in place to report on the Constabulary's fleet availability and downtime. These are currently being reported on Qlik Sense (Qlik) and to Senior Management at quarterly Transport Service Finance meetings. A performance dashboard is currently in the process of being implemented which will report these KPIs corporately. However, this is not yet in place.
- The arrangements between Bristol City Council (BCC) and the Constabulary surrounding the introduction of clean air zones by March 2021 have not yet been agreed. This is largely a result of delays BCC have had with the scheme. Whilst no formal recommendation has been raised around this area, management are asked to consider the findings and assure themselves that adequate arrangements are in place to address these once more information is known.

Application of Control Framework

The following issues were identified in the application of the control framework:

- Potentially due to the issues detailed above, fleet vehicles were found not to have been serviced or MOT’d within their required maintenance schedules / patterns. Of a sample of 20 vehicles reviewed, 13 were found to have expired services or MOTs. Some of these vehicles have since been serviced or MOT’d; however, others are still overdue and continue to be used for policing or business purposes. In one instance, a vehicle with an overdue service of six months was identified but is still in use. Whilst the majority of the Constabulary’s fleet vehicles will be serviced beyond the manufacturers stated requirement, there is a risk that some vehicles may be unroadworthy, unsafe or inefficient which could lead to void insurance, illegal use of the vehicle, financial loss, reputational damage, injury and/or death to an employee or member of the public.
- To assist with the scheduling system described above, vehicle owners are required to upload their vehicle mileage into Tranman weekly. However, over 100 vehicles were identified as not having a mileage reading uploaded in the last month. Over 40 of these vehicles had not had a mileage reading uploaded in the last year and some of these vehicles had not had a mileage reading upload since 2015. Going forward, this issue will largely be resolved by the telematics systems installed / planned to be installed in the Constabulary’s fleet vehicles.
- Data from Tranman which informs the KPIs above was assessed. We noted at least 50 instances of incorrect or incomplete dates (detailed further below) in the data reviewed. This will have an impact on the accuracy of both the availability and downtime information being reported on Qlik and to Senior Management. Given the negative impact that incorrect or incomplete data will have on the KPIs being reported, it is likely that Transport Services are actually operating at higher availability and lower downtime than what is currently being reported through Qlik. Inaccurate or misleading information reporting may lead to poor decision making which could result in financial loss and reputational damage to the Constabulary.
- There are also some instances where vehicles have not been collected by their owners within a reasonable timeframe after repairs or maintenance have been completed. There were over 35 cases where a vehicle had been collected after two weeks of work being completed. This may have an adverse impact on the Constabulary to deliver its operations could lead to dissatisfaction in the policing service, financial loss and reputational damage.

Audit Assessment of Agreed Themes

Theme	RAG Rating	Reason for RAG Rating
Leadership & Culture	🟩	Management within Transport Services are aware of a number of issues facing its service. The introduction of new processes and controls as highlighted in our conclusion above demonstrates the commitment of management to help resolve these issues and improve the service going forward.
Learning	🟧	Our review has highlighted some gaps in training (see Section 1.2 below) which has impacted on the RAG rating we have been able to provide in this area.
Diversity and Inclusion	Not Assessed	We have been unable to provide an opinion on diversity and inclusion specific to the processes reviewed.

Background

The Constabulary's fleet comprises of 1,071 vehicles. In addition, 167 vehicles are also hosted by the Constabulary on behalf of the other regional forces. The total value of the fleet is around £19.8m.

An Infrastructure Strategy is in place. The high-level goals and objectives set out within the five-year strategy will cover some aspects of work related to Transport Services and includes the following objectives:

1) We will deliver infrastructure that promotes and supports agile working > Developing our buildings and fleet to best support a modern, digitally-enabled and agile workforce with a visible policing presence in our communities
2) We will develop our assets to improve utilisation, sustainability, and value for money > through delivery of our 6 point sustainability plan and robust asset management to ensure our infrastructure supports the demands of modern policing
3) We will develop our working environment, equipment and facilities to support wellbeing, collaborative working and creative thinking > creating conditions that are inclusive and help maximise the productivity of our workforce
4) We will improve data quality and use of analytics across enabling service functions > improving the timeliness, accuracy and accessibility of information on our business support functions, and inform decision making
5) We will have relevant and credible professional support, advice and consultancy services in place > ensuring we use the right blend of internal and external expertise to allow effective decision making, ensure compliance, manage risk and maintain public confidence in our service.

Corporate Risk Assessment

Audit Objective

To provide assurance on the effectiveness of controls in place to manage, monitor and maintain the Constabulary's fleet to deliver its operational requirements. This will include a review of any work being undertaken to reduce the environmental impact of the Constabulary's fleet through the use of cleaner and more energy efficient vehicles.

Risk	Inherent Risk Assessment	Manager's Initial Assessment	Auditor's Assessment
Fleet vehicles are not managed, monitored and/or maintained effectively to meet operational, statutory or manufacturing requirements which could lead to financial loss, reputational damage, injury and/or death.	**High**	**High**	**Medium**

Scope

The audit considered the following:

- The Constabulary’s Fleet Management Strategy (or equivalent) which sets out its approach to effective fleet management. This forms part of the Constabulary’s Infrastructure Strategy, covered by the Refreshing the Strategic Framework report, provides some insight in this area.
- Services plans / maintenance schedules in place which outline roles, responsibilities, timescales and deliverables intended to reduce vehicle downtime. Due to the data quality issues identified by this review (discussed in Section 1.2), we did not assess whether actual performance was adequate to meet operational needs. This will need to be considered by Transport Services once underlying data quality issues are fully understood and resolved.
- The controls in place to manage and monitor the availability of the fleet to meet business needs.
- Performance management / Key Performance Indicators in place which inform decision making to help ensure effective fleet management.
- The measures in place to help reduce the environmental impact of the Constabulary’s fleet, including an assessment of the Constabulary’s readiness to meet compliance with the Clean Air Zones due to be implemented in Bristol and Bath by the end of 2021.
- Benchmarking information regarding the fleet management of our other Police Partners. The findings from this benchmarking will be reported separately.

Findings and Outcomes

1. Fleet vehicles are not managed, monitored and/or maintained effectively to meet operational, statutory or manufacturing requirements which could lead to financial loss, reputational damage, injury and/or death.	Medium

1.1 Finding and Action

Issue	Risk
Fleet vehicles are not being serviced or MOT'd within their required maintenance schedules.	Vehicles may be unroadworthy, unsafe or inefficient which could lead to financial loss, reputational damage, injury and/or death.

Findings

The Constabulary's fleet vehicles have each been assigned a maintenance schedule / pattern for servicing and MOTs. For example, a vehicle may require a service every 12 months or every 10,000 miles, whichever arrives first. Under the Motor Vehicles (Tests) Regulations 1981, the Constabulary is exempt from undertaking MOTs but must maintain their vehicles to a high standard in workshops approved by the Secretary of State. All fleet vehicles will therefore undergo an 'MOT' equivalent test each year.

A report detailing all vehicles that were out of service for repairs, servicing, MOTs etc. between June 2019 – December 2019 was provided as part of this review. Data analytics was used to identify vehicles in this period which may not have been serviced or MOT'd. A sample of 20 vehicles were reviewed to ensure that these had been serviced or MOT'd within their required maintenance schedules. 13 out of the 20 vehicles reviewed were found to have expired services or MOTs. Some of these vehicles have recently been serviced or MOT'd, others are still overdue a service or a MOT and continue to be used for policing or business purposes. The tables below provide a summary of our findings.

Table A: Fleet Vehicles with Expired Services

Fleet Number	Service Expired By	Current Status of Service
7330	6 Months	Not Started
7218	3 Months	Not Started
6304	2 Months	Not Started
6973	1 Month	Complete
5994	2 Weeks	Complete
6482	2 Weeks	Complete
7212	1 Week	Complete

Table B: Fleet Vehicles with Expired MOTs

Fleet Number	MOT Expired By	Current Status of MOT
6694	1 Month	Not Started
6749	1 Month	In Progress
6539	1 Month	Complete
5994	3 Weeks	Complete
6576	3 Weeks	Complete
6636	1 Week	Complete

The above findings were discussed with the Transport Insurance and Systems Officer. The root causes of the issues were identified and have been detailed below. The Constabulary manages maintenance scheduling both at a local and central level. At a local level, individual teams with fleet vehicles should have in place controls to monitor the maintenance of their own vehicles (e.g. through spreadsheets etc.) and schedule in services and/or MOTs when required. These local level controls were not reviewed as part of this audit.

At a central level, Transport Services are able to schedule vehicle servicing and maintenance through its Fleet Management System (Tranman). A weekly report is run which will check the last date a vehicle was serviced or MOT'd. The system will then estimate when the vehicle's next service or MOT is due. The Constabulary's central Admin Hub are responsible for sense checking this information manually to ensure that the vehicle has not already been serviced or MOT'd or scheduled in for one. Where a service or MOT is required, the Admin Hub will raise a job and notify the vehicle owner by email that their vehicle is due a service or MOT. It is then the responsibility of the vehicle owner to schedule and bring in the service or MOT. The Admin Hub will usually monitor these scheduling reports to ensure a vehicle has been booked in for work. However, monitoring has been affected by structural changes to the admin service incurred in autumn 2019. As result, some members of staff are new to the organisation / service and still learning processes. process. The actual scheduling of vehicles for servicing and MOTs is therefore reliant on the vehicle owner. As the process of emailing vehicle owners to schedule in their vehicles for a service or MOT is a manual one, there is an additional risk that these emails may not be being sent out to vehicle owners by the Admin Hub.

In addition to the above, once a report is run from Tranman to identify vehicles that are due a service or MOT and a job is raised by the Admin Hub, the system will assume that those vehicles with raised jobs have already been scheduled. These will then be excluded from any future reports produced unless the job is removed manually. As no monitoring occurs to ensure vehicles required a service or MOT are actually booked into a workshop for one, the default position is to exclude all vehicles with raised jobs from any future scheduling reports from Tranman. Therefore, some vehicles may miss their next service or MOT date if the vehicle owner does not schedule in the vehicle when initially prompted to do so and then subsequently forgets that one is due.

Furthermore, vehicle owners are required to upload their vehicle mileage into Tranman weekly. This information is used by the scheduling software to identify any vehicles that are approaching their mileage limit for servicing. Over 100 vehicles were identified as not having a mileage reading uploaded in the last month. Over 40 of these vehicles had not had a mileage reading uploaded in the last year and some of these vehicles had not had a mileage reading upload since 2015.

1.1a Recommendation		
We recommend that the Delivery Manager – Transport Services identifies all vehicles that have overdue services or MOT equivalents and ensures that these are undertaken as soon possible. A bespoke report from Tranman could possibly be produced to identify the last service and/or 'MOT' date of a vehicle and its next service or 'MOT' date. This information can then be analysed to identify any vehicles with overdue services or 'MOTs'.	Priority Score	2
Agreed Action	Timescale	01/05/2020

1. All overdue vehicles have been or are being removed from the road or have been serviced recently. 2. Transport Services are working on an updated report, in Qlik, to manage due/overdue vehicles. 3. Vehicle users / Facilities need to have local mechanisms to manage vehicle service/MOT due dates, it is the users responsibility to bring vehicles in for service on time.	Responsible Officer	Delivery Manager – Transport Services / Delivery Manager - Services Hub
1.1b Recommendation		
We recommend that the Delivery Manager - Transport Services investigates possible methods of automating the process of notifying vehicle owners that their vehicles are due a service or ‘MOT’. For example, where Tranman’s scheduling software identifies that a vehicle is due an ‘MOT’ or service, an email is automatically produced and sent to the vehicle owner instructing them to schedule in their vehicle for maintenance. Where the vehicle owner fails to schedule in the vehicle or instructs Transport Services otherwise, automated reminder emails should be sent to the vehicle owner requesting that they schedule the vehicle for a service or ‘MOT’ until the vehicle has been scheduled.	Priority Score	2
Agreed Action	Timescale	10/03/2021*
Transport Services and IBM have initially scoped the process to automate service/MOT notifications, we are now awaiting this to be formally documented and actioned by IT. *The IBM project manager has now moved on, A&S IT are recruiting somebody to pick this up, we do not have confirmation of date or our priority until they start.	Responsible Officer	Delivery Manager – Transport Services
1.1c Recommendation		
We recommend that the Delivery Manager - Transport Services investigates whether it is possible to update Tranman’s scheduling software to not automatically exclude a vehicle when a job has been raised for a service or ‘MOT’ from subsequent scheduling reports until it has actually been serviced or MOT’d.	Priority Score	3
Agreed Action	Timescale	01/05/2020
This would result in an unsustainable admin task for the Services Hub, in managing the deletion of old jobs, as each time the system generates a reminder it duplicates the record. This would be better managed by modifying the Qlik report in 1.1a.	Responsible Officer	Delivery Manager – Transport Services
1.1d Recommendation		
We recommend that the Delivery Manager - Transport Services, in liaison with the Delivery Manager – Estates and Facilities ensures all teams within the Constabulary with allocated fleet vehicles have adequate controls in place to manage and monitor the maintenance schedules of their vehicles at a localised level.	Priority Score	2
Agreed Action	Timescale	01/06/2020

The Delivery Manager – Transport Services to meet with the Delivery Manager - Estates, Facilities and Stores to review the local processes in place, that manage vehicle service/MOT dates to identify best practice and share across all sites.	Responsible Officer	Delivery Manager – Transport Services / Delivery Manager - Estates, Facilities and Stores

1.2	Finding and Action

Issue	Risk
Data quality issues within the Constabulary's Fleet Management system (Tranman) were identified. These were found to be a result of a combination of human error and/or omission and limitations with the system.	Inaccurate or misleading information may be reported to management which could result in poor decision making leading to financial loss and reputational damage.

Findings

Key performance indicators (KPIs) are in place to report on vehicle availability and downtime. The information is available on Qlik Sense (Qlik) and is reported quarterly at the Transport Finance meeting attended by Senior Management. Fleet availability is calculated in Qlik by identifying when work is in progress against a vehicle and therefore the vehicle is unavailable / inoperable. Vehicle downtime is calculated in Qlik by comparing the date when work on a vehicle commenced to the date when the job on a vehicle was completed. If work has not yet been completed on the vehicle, then Qlik will input the current date to calculate downtime.

A report detailing all vehicles that were out of service for repairs, servicing, MOTs etc. between June 2019 – December 2019 was provided for review. The information specifically used to report on KPIs was assessed for accuracy. The total number of days between when a vehicle arrived into a workshop for work (arrival date) and when work on the vehicle actually began (start date) were compared. This information informs the availability KPI reported in Qlik and to Senior Management as discussed above. Over 35 jobs were identified with 50 or more days between the arrival and start date. A sample of five of these were reviewed. In all five cases, it was identified that work had actually commenced earlier than the date entered on Tranman. As such, all five exceptions reviewed were found to be a result of human error.

In addition, the total number of days between the start date and when the work was completed on the vehicle (completed date) was also analysed. This information informs the downtime KPI reported in Qlik and to Senior Management. Over 45 instances where no start date had been entered were identified, resulting in Tranman calculating over 43,000 days between the start and completed date for these jobs (over 2m days in total). This would impact the accuracy of information being reported in Qlik and to Senior Management. In one instance, an end date in the future for December 2020 instead of 2019 had been entered into Tranman resulting in over 397 days between the start and end date for a job.

Due to the data quality issues identified above, our review did not assess whether actual performance was adequate to meet operational needs. This will need to be considered by Transport Services once underlying data quality issues are fully understood and resolved.

<table>
<tr><td colspan="4"></td></tr>
<tr><td>1.2a</td><td colspan="3">Recommendation</td></tr>
<tr><td colspan="2">We recommend that the Delivery Manager - Transport Services, in liaison with the Delivery Manager – Services Hub:
▪ Identifies common issues with data quality in Tranman;
▪ With appropriate assistance from other officers / Departments (e.g. Learning), develops a training programme, guidance and/or awareness around identified data quality concerns for all staff inputting data into Tranman; and
▪ Ensures all staff who actively input data into Tranman receive training to help ensure these issues are resolved and reduced going forward.</td><td>Priority Score</td><td>2</td></tr>
<tr><td colspan="2">Agreed Action</td><td>Timescale</td><td>30/06/2020 and 10/03/2021</td></tr>
<tr><td colspan="2">1. Transport Services to review and identify common data quality issues. The Delivery Manager – Transport Services to meet with the Delivery Manager - Services Hub to identify where training / support / documentation is required. (3mths)
2. Linked to replacing fleet software, we plan to utilise template jobs – to mitigate these issues. (12mths)</td><td>Responsible Officer</td><td>Delivery Manager – Transport Services / Delivery Manager - Services Hub</td></tr>
<tr><td>1.2b</td><td colspan="3">Recommendation</td></tr>
<tr><td colspan="2">We recommend that the Delivery Manager – Transport Services, with the assistance of CIVICA, investigates whether it is possible to update Tranman to ensure:
▪ A date has to be entered in all fields in Tranman before a job can be closed; and
▪ No future date can be entered into any field other than the ‘Booked in For’ field.</td><td>Priority Score</td><td>3</td></tr>
<tr><td colspan="2">Agreed Action</td><td>Timescale</td><td>10/03/2021</td></tr>
<tr><td colspan="2">Transport Services will investigate this issue, a resolution may be linked to the replacement of Tranman, if it is linked to that project then we will be waiting for up to 12 months.</td><td>Responsible Officer</td><td>Delivery Manager – Transport Services</td></tr>
<tr><td>1.2c</td><td colspan="3">Recommendation</td></tr>
<tr><td colspan="2">We recommend that the Delivery Manager – Transport Services, once data quality issues are fully understood, undertakes a data cleanse of Tranman. After this data cleanse has been performed, the Delivery</td><td>Priority Score</td><td>3</td></tr>
</table>

Manager – Transport Services should assess whether actual performance is adequate and if necessary, introduce further metrics / KPIs to determine and resolve root causes of any unsatisfactory performance.		🟧
Agreed Action	Timescale	10/03/2021
Tranman no longer support our version of the software, therefore no development is available on our version. We must replace our fleet management software in order to achieve this which we already have an RFS and live project with IT to achieve this year.	Responsible Officer	Delivery Manager – Transport Services

1.3	Finding and Action

Issue	Risk
Vehicles may not be collected by their owners within a reasonable timeframe after repairs or maintenance have been completed.	Vehicles that are ready to be deployed but are left uncollected in a workshop for an unreasonable amount of time may have an adverse impact on the Constabulary to deliver its operations. This could lead to dissatisfaction in the policing service, financial loss and reputational damage.

Findings
A report detailing all vehicles that were out of service for repairs, servicing, MOTs etc. between June 2019 – December 2019 was analysed to identify potentially unreasonable collection times of a vehicle after work had been completed. In four cases, no completed date had been entered but the vehicle had been collected and a collection date entered. This resulted a difference of over 43,000 days between completed and collected dates. A recommendation has been raised as part of Section 1.2 above to help address this issue. Other than these four cases, there were over 35 cases where a vehicle had been collected more than two weeks after work was completed.

1.3a	Recommendation

We recommend that the Delivery Manager – Transport Services, in liaison with the Delivery Manager – Estates and Facilities implements an escalation process which notifies vehicle owners that their vehicle is ready for collection at agreed intervals. For example, on the day work is completed, after 3 days and again after a week etc. A KPI could also be introduced into Qlik to better manage and monitor performance around completion to collection times / rates.	Priority Score	**2**
Agreed Action	Timescale	01/04/2020

Transport Services and the Facilities team already have plans in place to introduce a new process to allow vehicles not collected within 24 hours to then become eligible for volunteer drivers to return. This is at the stage of implementation.	Responsible Officer	Delivery Manager – Transport Services / Delivery Manager - Estates, Facilities and Stores

1.4	Findings
Bristol City Council (BCC) are due to implement a clean air zones (CAZ) in some parts of the city by March 2021. This will see a ban on privately owned diesel vehicles and a charge for commercial vehicles entering these zones. The Constabulary are likely to be exempt from the March 2021 deadline. However, a separate agreement will need to be reached with BCC to ensure compliance with CAZ by a certain date. This has yet to be agreed between BCC and the Constabulary due to delays BCC have incurred in finalising their proposed plans. As the agreement is reliant of BCC to finalise their proposed plans, no formal recommendation has been raised in relation to this area. The findings have been included for managements information. CAZs are also being introduced in Bath. A Memorandum of Understanding which sets out the Constabulary's commitment to ensuring compliance with the CAZ is already in place between the Constabulary and Bath and North East Somerset Council. The Constabulary anticipates that, by the time the CAZs are introduced in Bath, all fleet vehicles will be compliant.	

Authors and Distribution

Please note that this report has been prepared and distributed in accordance with the agreed Audit Charter and procedures. The report has been prepared for the sole use of the Partnership. No responsibility is assumed by us to any other person or organisation.

Report Authors

This report was produced and issued by:

Laura Wicks	Assistant Director – Emergency Services
Juber Rahman	Senior Auditor

Distribution List

This report has been distributed to the following individuals:

Benjamin Mohide	Delivery Manager – Transport Services
Richard Vise	Delivery Manager - Estates, Facilities and Stores
Teresa Leadbetter	Delivery Manager - Services Hub
Mark Simmons	Interim Chief Executive Officer
Nick Adams	Chief Finance Officer, Avon and Somerset Constabulary and OPCC
Jane Walmsley	Inspection and Audit Co-Ordinator
Helen Graham	Services Improvement Co-Ordinator

AVON & SOMERSET POLICE & CRIME COMMISSIONER

SWAP INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

6e

Avon and Somerset Police

Data Quality Training

Final Report

Issue Date: 10 March 2020

Working in Partnership to Deliver Audit Excellence

Executive Summary

Audit Opinion

Partial
Reasonable
Substantial
None

Partial

In relation to the areas reviewed and the controls found to be in place, some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.

Recommendation Summary

Priority	Number
Priority 1	**0**
Priority 2	**5**
Priority 3	**0**
Total	**5**

Audit Conclusion

Effectiveness of Control Framework

The Force is aware of weaknesses in the quality of its data and a risk is on the Strategic Risk Register to this effect. As such, we were requested to consider the training arrangements and processes in place surrounding NICHE and its feeder systems, which include the Force's command and control system (STORM) and its mobile interface which directly inputs data into NICHE (Airpoint). It should be noted that an ineffective training programme will not be the only cause of data quality issues and that the findings of this report ought to be reviewed in conjunction with other programmes of work aimed at improving data quality.

At the time of the audit, there were over 215,000 crime recording and file quality errors assigned to 4,000+ individuals and over 600,000 duplicate records by people, addresses, vehicles and phone numbers still to be resolved. 1,100 errors had been assigned to a single individual. A large volume of unusable police information is also present within NICHE. Whilst we acknowledge that a significant proportion of these errors will have been inherited by NICHE from legacy systems, these errors continue to increase faster than they can be resolved by the Records Retention Team (RRT). The RRT is in place to address errors manually and are responsible for resolving over 12,000 errors per month.

Given the number of errors outlined above, the Force is seeking to take action to improve the culture around data quality and highlighting the importance of data across the organisation. Some of these actions are outlined below, however these are yet to achieve a positive impact and errors continue to occur at a high rate. With establishment levels across the whole organisation likely to increase as a result of the Government's commitment to uplift police officer numbers by 6,000 (c.300 police officers for Avon and Somerset Police) by the end of March 2021 it is important that the pervasiveness of data quality issues urgently reduces and this will require training issues to be addressed as soon as possible, to help drive forward the desired culture of the Force in achieving data quality.

Design of Control Framework

- NICHE training is covered within various training courses and programmes offered by the Force which is customised dependent on the role of the individual. NICHE training was first delivered in 2015 to police officers and staff following its initial roll out. Mandatory upskill training was then delivered following an update to NICHE in 2017. All police officers are required to complete NICHE training as part of their initial training. It is the responsibility of line managers to ensure any members of staff using NICHE receive training.

- No refresher training is currently being delivered to police officers and staff on NICHE. However, the Force are in the process of introducing refresher training for all Police Constable Degree Apprenticeship (PCDA) graduates following their two-year probation period. The arrangements for this have yet to be finalised.
- The current mechanisms in place to ensure data quality errors are resolved and appropriately managed and monitored on an individual basis require improvement. There are insufficient controls in place to hold officers and staff accountable for the quality of data input either personally or via line managers.
- Unusable police information records are being created in NICHE, which are currently not being reported back to the individual who created the record for resolution (e.g. through Qlik).
- Feedback in relation to NICHE training delivered by the Force is currently being gathered from PCDA students. This feedback will help the Force improve the training programme delivered to its police officers. However, the Force does not currently obtain feedback from NICHE courses delivered internally that are usually completed by smaller groups of individuals.

In recognition of work needed to address risks around poor data quality, the Force has set up the following:

- Data quality is discussed quarterly at meetings of the Strategic Information Management Board (SIMB). This forum is chaired by the Deputy Chief Constable.
- A Data Quality Task and Finish Group meets bi-monthly to discuss data quality across the organisation. This is attended by representatives from Learning, IT and the Records Retention Team (RRT) and is chaired by an Assistant Chief Constable. The work undertaken as part of this group will be fed back to SIMB.
- Technological / automated solutions are being developed with IBM and NICHE to help resolve data quality errors.
- Police officers and staff with assigned crime and file quality errors are able to resolve these through the ‘My Work’ application in Qlik Sense (Qlik).
- Data quality concerns are being communicated force-wide through newsletters, blogs and intranet pages.
- A request for the introduction of mandatory fields to be added into NICHE has been made to the developers of NICHE. These will help ensure a minimum information requirement for police records. However, the development and implementation of these have been delayed as a result of other priorities (e.g. the roll out of NICHE v.6 due to be implemented in summer 2020).

Application of Control Framework

A minimum of 890 individuals with data quality errors assigned to them in NICHE do not appear to have received any training on how to use the system. There are potentially further individuals who may also not have received training on NICHE, which could be negatively impacting data quality. It should be noted that only a proportion of the workforce will be required to use NICHE.

The top 25 individuals with the highest number of crime recording and file quality errors (6% of the total errors) were reviewed to ensure that these individuals had received formal training on NICHE or associated systems. Two of the 25 individuals were found to have not received any initial NICHE training delivered in 2015 following the roll out of NICHE. One other individual was found to have only received the initial training in 2015 but not mandatory upskill training in 2017 following a major update to NICHE that year.

In addition, a report from Qlik detailing the highest number of data quality errors by specific Teams was provided by the Business Objectives Team for review. Six of the top 10 Teams with the highest number data quality errors had not received any refresher training. The impact of this training has yet to be realised.

Audit Assessment of Agreed Themes

Theme	RAG Rating	Reason for RAG Rating
Leadership & Culture	🟧	Data quality risks are recognised at the highest level of the organisation. However, the RAG rating we have been able to offer in this area has been impacted by the volume of poor data currently held in NICHE. These cannot be resolved without strong leadership and a cultural shift in how police officers and staff view the importance of data quality.
Learning	🟧	Our review has highlighted potential gaps in training (see Section 1.1 and 1.2 below) which has impacted on the RAG rating we have been able to provide in this area.
Diversity and Inclusion	Not Assessed	We have been unable to provide an opinion on diversity and inclusion specific to the processes reviewed.

Background

Data quality errors within the Force's records management system (NICHE) is a well-recognised risk and is included within the Force's Strategic Risk Register. Data quality within the Force is outlined into three main areas:

1. Crime recording and file quality which the user can resolve and is highlighted within Qlik;
2. Duplicate entities including people, objects, location and events (also known as POLE). This area is considered by the Force to be too high risk to allow individuals to rectify and therefore, is currently resolved by the RRT; and
3. Unusable police information which is information that does not conform minimum standards. For example, person entities without a date of birth or an address without a post code. This area is currently resolved by the RRT.

NICHE training is covered within various training courses and programmes offered by the Force. The training course delivered is dependent on the role of the individual. The main training courses which cover NICHE are as follows:

- Niche for the Incident Assessment Unit (IAU)
- Niche Op User (for Police Officers)
- Niche 5.04 (for IAU and Op Users)
- Niche training for PCSOs, Special Constables and Transferees (three separate courses)
- Niche Two Way Interface Training which was mandatory for all individuals using NICHE
- Police officers recruited from the Initial Police Learning and Development Programme (IPLDP) that was completed after 2015 which would have included NICHE training
- Police officers recruited from Police Now graduate programme that was completed after 2015 which would have included NICHE training.
- Police officers recruited from the Police Constable Degree Apprenticeship programme which includes NICHE training

In addition to these main courses and programmes which cover NICHE, smaller / more bespoke NICHE training courses are also in place which have been completed by fewer individuals.

Corporate Risk Assessment

Audit Objective

To provide assurance over the effectiveness of the Force's training programme in place to help ensure the accuracy and completeness of data captured within its records management system (NICHE) and that the Force is seeking to drive a positive culture around data quality.

Risk	Inherent Risk Assessment	Manager's Initial Assessment	Auditor's Assessment
Poor data quality could negatively impact the effectiveness, efficiency and credibility of the Force's operations, planning, decision making and crime outcomes. This could result in the safety of the public being compromised, financial loss, reputational damage, legal challenge and/or loss of confidence in the policing service.	High	High	Medium

Scope

Given the work already undertaken in this area to help mitigate the risks that poor data quality presents to the business, it was agreed with Senior Management that SWAP would review and provide an opinion over the effectiveness of the Force's training programme to help prevent data quality errors going forward. The audit therefore considered the following:

- The effectiveness of the training programme / strategy in place for police officers and staff which sets out practices aimed at ensuring high quality of information within NICHE (including training surrounding the use of any systems which feed information into NICHE e.g. STORM, AirPoint etc.). This included a review of the content to ensure that it covers data quality errors facing the Force specifically and whether the training highlights the potential consequences / risks of inaccurate or incomplete data capture.
- The mechanisms in place to inform and review the training programme surrounding data quality. This included an assessment on whether participant feedback is being acted upon and new or emerging issues are being considered.
- Controls in place to ensure compliance with training requirements. Data analytics was used to compare three different sets of data in order to identify individuals who may not have completed NICHE training:

  1) All individuals with assigned crime recording and file data errors within NICHE (exported from Qlik in early February 2020)
  2) All individuals who have completed one or more of the main training courses and programmes which cover NICHE (exported from LSO in mid-February 2020)
  3) All police officers and staff (exported from SAP in November 2019 as part of our Payroll and Expenses audit)

  Due to the differences between all three reports, we were unable to confirm the training status of some individuals (see Section 1.1 below).
- The mechanisms in place to review, report and resolve data quality errors that are a result of human error or omission. This included an assessment on the effectiveness of governance and oversight controls in place to prevent, reduce and resolve data quality errors.
- Any work undertaken by the Force to promote the importance of data quality across the organisation.

Findings and Outcomes

1. **Poor data quality could negatively impact the effectiveness, efficiency and credibility of the Force's operations, planning, decision making and crime outcomes. This could result in the safety of the public being compromised, financial loss, reputational damage, legal challenge and/or loss of confidence in the policing service.**	**Medium**

1.1 Finding and Action

Issue	Risk
Some police officers and staff who input data into NICHE and other systems which feed information into NICHE (e.g. Airpoint, STORM etc.) may not have received any training on how to use these systems.	Input of poor data which could negatively impact the effectiveness, efficiency and credibility of the Force's operations, planning, decision making and crime outcomes.

Findings

A report of all individuals who have completed the main NICHE training courses and programmes (detailed within the 'Background' section above) was exported from the Force's Learning System (currently LSO which is due to be replaced by Chronicle). The information was compared to a report of all individuals with assigned crime recording and file quality errors (referred to hereafter as data quality errors) exported from Qlik Sense (Qlik). Over 870 individuals were found not to have completed one or more of the main NICHE training courses or programmes.

A summary has been provided in the tables below:

Table A: Summary by Role

Role*	Total
Police Staff	556
Police Officers	213
PCSOs	70
Special Constables	58
Grand Total	**897**

Table B: Summary by Start Date

Year	Total
1979 – 2014 (prior to NICHE)	479
2015 – 2019	398
Sub Total	**877**
Unable to Confirm*	20*
Grand Total	**897**

**20 Individuals were found not to have a start date inputted against their record within SAP. Therefore, we were unable to confirm their start dates. Job roles are accurate as of November 2019.Therefore, any internal movement between job roles after November 2019 will not be accounted for in the totals provided.*

It is worth noting that there are more bespoke training courses and programmes that include NICHE training other than the main ones detailed within the 'Background' section of this report. However, these are only delivered to a limited number of individuals and therefore there is a possibility that some of the individuals identified above may have attended a bespoke course not captured by our analysis. Our findings also do not take into account potential data quality

issues with the information held in LSO. As such, our findings may have identified some instances where NICHE training has actually been completed by an individual, but this has not been recorded in their LSO record due to input error or omission. In addition, a sample of the top 25 individuals with the highest number of data quality errors was reviewed to ensure that these individuals had received formal training on NICHE or associated systems. Two of the 25 individuals were found not to have received the initial NICHE training delivered in 2015 following its roll out. However, both individuals had received upskill training in 2017 following a major update to the system (NICHE 5.04). The upskill training only focused on specific elements that had been added to the update and were not included in the previous version rolled out in 2015 and was mandatory for all individuals using NICHE. One other individual from our sample was found to have only received the initial training in 2015 but not the upskill training in 2017. Whilst the other 22 individuals were found to have received NICHE training in 2015 and 2017, there appears to be a significant number of data quality issues occurring and as such, these individuals would benefit from further training.		
1.1a Recommendation		
We recommend that the Chief Officer – People and Organisational Development conducts a full investigation into the exceptions identified by our analysis and ensures all individuals identified in our report have completed NICHE training. In instances where individuals are found not to have completed NICHE training, the Head of Learning should ensure relevant NICHE training is completed by these individuals at the earliest opportunity.	Priority Score	2
Agreed Action	Timescale	31/12/2020
Work is currently in place in order to develop a training package that supports those officers on PCDA, Supervisors and those in need of further development. The data identifying those who are making common or impactive errors or those who have not attended recent training will be used to target those most in need of development. Some will be invited to the scheduled Operational Users two/three-day training course or will receive bespoke training designed to develop the areas of weakness.	Responsible Officer	Head of Learning
1.1b Recommendation		
We recommend that the Chief Officer – People and Organisational Development ensures that NICHE refresher training is provided to all individuals who are considered to have an unacceptable amount of data quality errors assigned to them in Qlik. Mechanisms should also be put in place to monitor individuals that receive refresher training to ensure their performance is satisfactory going forward.	Priority Score	2
Agreed Action	Timescale	31/12/2020
As above action, plus work is being conducted with Business Improvement to develop a compliance app specifically for this. This will enable both team supervisors and training to quickly identify those who need further support.	Responsible Officer	Head of Learning

1.2 Finding and Action

Issue	Risk
Some Teams with high levels of data quality errors assigned to them have not been provided with refresher training.	Input of poor data which could negatively impact the effectiveness, efficiency and credibility of the Force’s operations, planning, decision making and crime outcomes.

Findings

A report from Qlik detailing the highest number of data quality errors by specific Teams was provided by the Business Objectives Team for review. Internal training is currently being delivered by the Records Review Team (RRT) to Teams found to have a high number of data quality errors assigned to them. Out of the top 10 Teams with the highest number data quality errors, four have been provided with refresher training by the RRT. No training has been scheduled for the other six Teams. A summary has been provided in the table below:

Team	Total Number of Data Quality Errors	Date of Refresher Training
Desktop IAU Team 3	5,123	28/11/2019
Desktop IAU Team 1	4,990	22/01/2020
Desktop IAU Team 4	4,330	21/11/2019
Desktop IAU Team 4	4,257	15/01/2020
Team 1 Patrol Base 4	3,110	Not scheduled
Team 2 Patrol Base Concorde	2,894	Not scheduled
Team 4 Patrol Base 2	2,704	Not scheduled
Team 3 Patrol Base 3 Broadbury	2,030	Not scheduled
Op Remedy Team 2	1,930	Not scheduled
Team 1 Patrol Base 1 Patchway	1,882	Not scheduled

The RRT are currently in the process of reviewing whether the refresher training they have delivered to the above Teams has had any impact on the reduction of data quality errors generated by those Teams specifically. Once analysed, a report will be submitted to the Data Quality Task and Finish Group highlighting the key findings.

1.2a Recommendation

We recommend that the Chief Officer – People and Organisational Development mandates that refresher training is provided to all Teams that are considered to have an unacceptable level of data quality errors assigned to them in Qlik. Mechanisms should also be put in place to monitor Teams that receive refresher	Priority Score	2

training to ensure their performance is satisfactory and underlying issues with data quality are addressed going forward.		
Agreed Action	Timescale	31/12/2020
The Record Review Team manager will work with the Head of Learning to identify where a need for training is apparent according to the data on teams, who have an unacceptable level of data quality errors. This process can also highlight where training will not be able to address the DQ errors caused but other interventions needed, such as Technology or new processes. Performance and a possible feedback strategy will be managed via the Data Quality strategic group, with governance and support from an assistant chief constable. The Qlik Sense application will be used by RRT to provide a report on progress.	Responsible Officer	Records Review Manager and Head of Learning

1.3	Finding and Action

Issue	Risk
The current mechanisms in place to ensure data quality errors are resolved and appropriately managed and monitored on an individual basis may not be effective.	Input of poor data into NICHE and other systems could negatively impact the effectiveness, efficiency and credibility of the Force's operations, planning, decision making and crime outcomes.

Findings
Qlik will identify any missing / incomplete information within the crime recording database in NICHE. For example, where an MO has not been entered. Any missing or incomplete information will be classified as a data quality error and reported back to the individual who generated the record through the ‘My Work application in Qlik. All individuals with data quality errors assigned to them will be required to rectify these. It is the responsibility of these individuals and their line managers to ensure data quality errors are resolved. However, given the high number of data quality errors currently held (over 215,000), the Force needs to introduce more effective processes and procedures to ensure individuals take ownership of their data quality errors. In addition, the Force should implement more robust supervisory controls to manage and monitor data quality performance on an individual basis going forward.

1.3a	Recommendation	
We recommend that the Chief Officer – People and Organisational Development, with direction from other appropriate officers, implements a process which ensures greater accountability for data quality and introduces measures to monitor and manage data quality on an individual basis. Data quality could for example form part of someone’s Individual Performance Record or appraisal process. Performance surrounding the rectification of data quality errors should also be regularly reported at a corporate level (e.g. to the Strategic Information Management Board) and appropriate action taken in areas deemed to be unsatisfactory.	Priority Score	**2**

Agreed Action	Timescale	31/12/2020
RRT manager accepts the recommendation and will consider the plan to address this at the next DQ Task and Finish group for consultation with force stakeholders for possible IPR input and monitoring. A plan will be established and implemented to bring about greater accountability by the next Strategic Information Management Board in Q3 2020.	Responsible Officer	Records Review Manager

1.4	Finding and Action

Issue	Risk
Unusable police information errors are being created in NICHE and not fed back to individuals generating them.	Input of poor data into NICHE and other systems which could negatively impact the effectiveness, efficiency and credibility of the Force's operations, planning, decision making and crime outcomes.

Findings
Unusable police information are records created that are not reliable enough to make policing decisions. For example, the creation of entities without a date of birth, address and/or post code. These are currently not being reported back to the individual who created the record for resolution (e.g. through Qlik). The Records Retention Team are instead responsible for resolving these issues. Work is underway to reduce the number of these records including through the use of technological solutions (e.g. Niche Autograder and MDM). In addition, the Force has also requested mandatory fields to be added into NICHE which will ensure a minimum standard of information in NICHE. However, development of these has been delayed due to the roll out of the new version of NICHE due to be implemented in summer 2020. Whilst we acknowledge the work of the Records Retention Team in this area, unusable police information will continue to be created unless a method is introduced to identify the individuals creating these records and preventative action is taken to address the root cause of the problem.

1.4a	Recommendation

We recommend that the Chief Officer – People and Organisational Development implements a method of identifying individuals and Teams who create unusable police information. Once identified, measures should be taken to help prevent these individuals and Teams from creating unusable police information. For example, through retraining.	Priority Score	2
Agreed Action	Timescale	31/12/2020
RRT will identify a means of analysing the causes of those creating unusable police information and of targeting action to mitigate this risk. Development in IT tools will have to be explored to support this and the analysis and plan will be considered by the SIMB for approval by strategic Information Management Board in Q3 2020.	Responsible Officer	Records Review Manager

Other Suggestions
The Force is currently in the process of obtaining training feedback from police officers recruited under the Police Degree Apprenticeship Programme (PCDA). Feedback will first be reviewed by the Force's programme delivery partner (the University of West England (UWE)) before being analysed by the Force's Learning Department. Whilst feedback has yet to be fully gathered by UWE, the Force should ensure, once feedback is received, that it is fully analysed, and improvements are made in areas of concern. This should include a thorough analysis of any feedback obtained in relation to the NICHE training modules delivered as part of the PCDA. The Force does not currently obtain feedback from NICHE courses delivered internally that are usually completed by smaller groups of individuals. Management should consider gathering feedback from these smaller courses in addition to its larger ones such as the PCDA.

Authors and Distribution

Please note that this report has been prepared and distributed in accordance with the agreed Audit Charter and procedures. The report has been prepared for the sole use of the Partnership. No responsibility is assumed by us to any other person or organisation.

Report Authors

This report was produced and issued by:

Laura Wicks	Assistant Director
Ed Nichols	Principal Auditor
Juber Rahman	Senior Auditor

Distribution List

This report has been distributed to the following individuals:

Sarah Crew	Deputy Chief Constable
Daniel Wood	Chief Officer – People and Organisational Development
Mike Carter	Head of Learning
Nick Lynn	Records Review Manager
Mark Simmonds	Interim Chief Executive Officer
Nick Adams	Chief Finance Officer, Avon and Somerset Police and Interim Chief Finance Officer, OPCC
Jane Walmsley	Inspection and Audit Co-Ordinator

AVON & SOMERSET
POLICE & CRIME COMMISSIONER

SWAP
INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

6f

Avon and Somerset Police
Refreshing the Strategic Framework

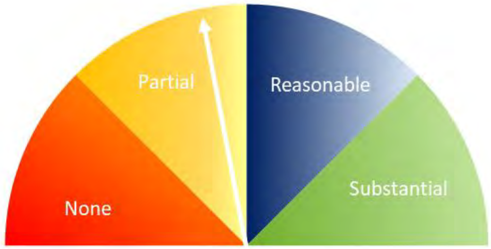
Final Report

Issue Date: 10 March 2020

Working in Partnership to Deliver Audit Excellence

Executive Summary

Audit Opinion



Partial

In relation to the areas reviewed and the controls found to be in place, some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.

Recommendation Summary

Priority	Number
Priority 1	**0**
Priority 2	**3**
Priority 3	**5**
Total	**8**

Audit Conclusion

Effectiveness of the Control Framework

The Force has made considerable progress in implementing its refreshed Strategic Framework during the last 18 months and is looking to deliver change, the need for which was recognised by all stakeholders interviewed as part of the audit. It was clear that certain elements of the Framework had 'landed' better than others; for example, the values, vision and mission, together with the four corporate strategies. The strategic planning cycle over the course of the year is delivering benefits in ensuring plans are completed and reviewed at the right time, with further understanding of the interdependencies of these plans on each other. The cycle of meetings has further aided the governance structure under the Framework in assisting information flow across the organisation.

However, weaknesses were identified across a number of areas and closure of the project was not achieved as intended by July 2019, mostly due to the WeKan system not being able to support the Single Delivery Plan. Work to address this remains ongoing at the time of the audit and depending on the date the proposed new solution becomes available, closure of the project is now not expected until Summer 2020, with a planned Post Implementation Review to follow in December 2020. In addition, benefits around streamlined governance have not yet been achieved and risk management arrangements could be strengthened. These are elaborated on below.

Whilst there are a number of recommendations within this report, several of these have been raised with a view to assisting the Force in maximising the benefits achieved in embedding its Strategic Framework. The main factors ultimately influencing our assurance opinion are those outlined above.

Design of the Control Framework

We consider the design of the control framework to be generally sound, supported by the Blueprint which is a comprehensive document outlining the journey the Force is seeking to take in making improvements to its strategic management processes. We identified the following areas of strength:

- Four corporate strategies - Service, People, Infrastructure and Digital - have been produced to support the delivery of the Strategic Framework. These are subject to annual refresh as a result of the contextual analysis completed (further expanded upon below).
- The Strategic Framework has been managed as a project, with a project team overseeing implementation and delivered by a Project Manager.

- The concept of a Single Delivery Plan to capture all areas of improvement activity across the Force to underpin delivery of the Framework.
- Engagement and consultation were commented upon by all stakeholders interviewed as satisfactory. Examples of corporate communications were requested but due to time constraints, these had not been received at the time of writing.
- Diversity and Inclusion is not a specific part of the Framework per se, however a Diversity and Inclusion Board forms part of the Constabulary Management Board meetings on a quarterly basis. Results of the People Survey demonstrate increased positive perceptions around inclusion.
- Governance arrangements were well designed, with template Terms of Reference outlined in the Blueprint which require objectives, inputs, processes and outputs to be detailed. A governance structure was also detailed to support information flow throughout the organisation.

There were some areas of weakness/areas which could be improved upon within the design of the control framework as follows:

- Risk Management appeared to be overcomplicated as per the most recent version of the Blueprint provided. This was now going through an internal review. In addition, recommendations to consider the wording of the proposed strategic risks, links between Directorate/operational level risk management and roles and responsibilities have been raised to support the review.
- Due to the delays in the project, mainly due to WeKan (expanded upon below), the Framework as a project has not been delivered for Business as Usual within the initial timeframe expected. It was not clear as yet whether a formal handover plan was in place, outlining roles and responsibilities for managing/overseeing the Framework once complete.
- Finally, there are a number of benefits outlined within the Blueprint, however these are not wholly SMART. A recommendation has been raised regarding this as whilst the focus has been on making Objectives SMART, this has not occurred with the benefits expected to be derived from implementing the Framework. At present, these lack tangibility and would be rather subjective when covered by a Post Implementation Review.

Application of the Control Framework

WeKan is the system that the Force sought to use to manage its Single Delivery Plan. During late summer/autumn 2019, it was decided that WeKan was unable to provide the capability to deliver the SDP, despite there being work completed on the functionality required by the solution, including a 'requirements list' which detailed the 'must-haves' for the system. The volume of data required to manage the SDP was not wholly clear and WeKan was unable to cope with the data. Upgrades to WeKan were deployed and despite server power increases, the system was still unable to function as intended. Further details are outlined in Section 1.1 below.

Due to being unable to utilise WeKan, the Force has reverted to using spreadsheets to record improvement plans for the Directorates, which our sample audit testing identified as being subject to regular review and update, though not all formats in use were the same. The intention is that all Directorate improvement plans are to be amalgamated in April 2020 and this will form the interim basis for reporting upon the SDP. This option also allows for visualisation through Qlik, the Force's performance management suite, so the ultimate experience is not altered despite the background data coming from a difference source.

Stakeholders interviewed during the course of the audit felt that the streamlining of governance mechanisms had not yet been fully embedded, and they felt they were still attending as many meetings, many of which were somewhat duplicated. Opinions from stakeholder interviews noted that the Senior Leadership Meetings (SLM) were not as effective as intended and many Terms of Reference for meetings detailed in the governance structure were incomplete. A review of governance was confirmed to have started towards the end of our audit.

Arrangements for review of the Strategic Risk Register (SRR) had changed from those outlined in the Blueprint. The Constabulary Management Board was the intended recipient of the SRR and was required to consider this on a monthly basis. This has now been moved to the remit of the Strategic Planning Meeting (SPM) which takes place on a quarterly basis as this was felt to be the most appropriate forum (membership of the two groups is very similar).

Audit Assessment of Agreed Themes

Theme	RAG Rating	Reason for RAG Rating
Leadership & Culture	🟩	The design of the Blueprint in particular is considered effective and all stakeholders interviewed during the course of the audit commented upon the embeddedness of the Force’s values, Vision and Mission. It is clear that significant progress has been made on the Force’s journey with progressing its new Framework, which is down to effective leadership. The new culture, particularly around meetings, will take time to embed; however, the intention is very much clear to drive streamlined governance across the organisation.
Learning	Not Assessed	Learning has not been specifically assessed as part of this review. Commentary is provided within the Blueprint around learning, however this was outside of the scope of this audit.
Diversity and Inclusion	🟩	Diversity and Inclusion is not a specific part of the Framework per se, a Diversity and Inclusion Board forms part of the Constabulary Management Board meetings on a quarterly basis. Results of the People Survey demonstrate increased positive perceptions around inclusion.

Background

The Strategic Framework (SF) is a single, enabling framework and set of principles that will be used universally across Avon and Somerset Police (ASP) for defining strategy, developing delivery plans, undertaking corporate planning, and facilitating innovation, improvement and transformation activity at all levels.

A short piece of scoping work conducted in August 2018 demonstrated the tangled strategic environment that had evolved within the organisation. At that time, the organisation had at least 14 different strategies, around 70 plans and over 2,000 actions. This resulted in over 30 regular corporate meetings, taking up over 9,500 hours and costing c.£430k per annum.

A new mission, vision and values for the Force were developed and launched at the end of 2018, it was identified as critical to take the opportunity to declutter the landscape and ensure that there was a clearer framework to help deliver that vision. The ‘Strategic Framework Project’ was established in October 2018 to develop a Blueprint for how this would be achieved.

Corporate Risk Assessment

Objective

To provide assurance on the Force's current position in developing and implementing its refreshed strategic framework, including the embeddedness of diversity and inclusion therein.

Risk	Inherent Risk Assessment	Manager's Initial Assessment	Auditor's Assessment
The Force does not achieve the objectives set, fails to realise the benefits from and/or fails to embed diversity and inclusion within its revised strategic framework, leading to potential inefficiencies, weakened governance, non-delivery of Force Strategies, Single Delivery Plan, lack of value for money and lack of progress of the Force's agenda around diversity and inclusion.	**High**	**Medium**	**Medium**

Scope

The audit considered the following:

- The blueprint/project plan and documented approach to the new strategic framework;
- Refreshed Mission and Vision;
- Strategies developed/in the process of development underpinning the framework;
- Objectives/benefits of the framework;
- Single Delivery Plan;
- Delivery of the Framework;
- Stakeholder engagement;
- Governance, assurance and links to risk management under the new framework; and
- The embeddedness of diversity and inclusion in the new framework.

Testing to verify the actions and assurance in the Single Delivery Plan was not completed, due to the issues outlined within this report and the infancy of its introduction. We have also not considered Business as Usual / compliance activity which would sit alongside the Strategic Framework as this sits more within the Force's performance framework, which is proposed for audit coverage in 2020/21.

Findings and Outcomes

1.	**The Constabulary does not achieve the objectives set, fails to realise the benefits from and/or fails to embed diversity and inclusion within its revised strategic framework, leading to potential inefficiencies, weakened governance, non delivery of Force Strategies, Single Delivery Plan, lack of value for money and lack of progress of the Force's agenda around diversity and inclusion.**	**Medium**

1.1 Finding and Action

Issue	Risk
The use of WeKan to provide the technical solution for the Single Delivery Plan has not worked as intended, meaning this element of the Strategic Framework has not currently been delivered.	Objectives within the strategies are not realised as intended, delaying the benefits desired from the new Strategic Framework.

Findings

According to the Blueprint, an integral part of the Force's Strategic Framework is the implementation and use of a Single Delivery Plan (SDP) which is the result of a successful strategic planning cycle and is considered an iterative process. The SDP brings together all of the improvement and change activities underway or planned across the Organisation into a single repository. This includes all activity to:

- Meet the organisation's strategic objectives and support the Mission, Vision and Values of the Force;
- Respond to changes in the internal or external environment (e.g. National legislative changes); and
- Respond to recommendations from HMICFRS inspections and other audit and assurance activity.

The Force sourced an IT solution called WeKan to support the delivery of the SDP. The Force was seeking an enterprise solution to manage all of its plans and actions. WeKan is a free solution and the Force's internal Development Team sought to adapt it to meet the needs of the business in delivering on the SDP and Strategic Framework. The WeKan system provides the underpinning data to then be presented by Qlik, the Force's performance management software, in order to make the data more accessible and would allow for 'slicing' the information in a variety of ways. WeKan is an 'open-source' product, which means that it is subject to regular updates from the online community. Once it is downloaded, that is the version that is taken and subsequently worked upon internally, whilst the online version is updated two or three times a day.

The IT Department worked with the Project Team to 'flesh out' and build a requirements list which detailed the functionality required from the system, including system 'must-haves' prior to proceeding to acquire WeKan. The Blueprint also contains information about the user requirements and responsibilities, which outlines what various levels of users would look to use WeKan for, though specific numbers are not detailed.

During late summer/autumn 2019, it was decided that WeKan was unable to provide the functionality/capability to deliver the SDP as intended. The system essentially would freeze, preventing access to and update of the actions therein. This was discussed with the Head of Transformation and the Head of Strategic Digital Services who both confirmed that the requirements around the volume of information to be captured and detailed within WeKan were not fully clear. It was intended that WeKan would use the "Kanban" (lean project methodology) approach of cards moving across a board and then being archived. The cards are larger pieces of information with checklists attached and given the nature of improvement actions, take some time to be in a position for archiving. As a result of the significant amount of data held on WeKan, the browser struggled to cope and rendered the solution impossible to use. To try and enable the system to work, the Development Team also obtained an updated version of WeKan, downloaded and deployed this and despite server power increases, this only resulted in limited improvement in usability.

The Head of Transformation acknowledged the lessons learned from the attempted deployment of WeKan. As referenced above, the Force may not have been fully clear about / fully appreciated the volume of information required to be held on the system. Testing of the capability of WeKan could have been improved by forcing it to handle more data than was tested as part of this process. Furthermore, the Head of Transformation queried whether the Force had tried for too long to seek a workable solution with WeKan and whether this should have been ceased sooner.

Due to being unable to utilise WeKan, the Force has reverted to using spreadsheets to record improvement plans for the Directorates, which our sample audit testing identified as being subject to regular review and update in this way. The intention is that all Directorate improvement plans are to be amalgamated in April 2020 and this will form the interim basis for reporting upon the SDP. As part of our testing, we noted that some Directorate SDPs were maintained in a different format to others; however, with the amalgamation of all SDPs planned to take place, we have not raised a recommendation regarding this.

The Microsoft Office 365 suite is in the process of being rolled out nationally across police forces, including to Avon and Somerset. As part of this suite, there is a product called Microsoft Planner and the intention is to move to this when Microsoft 365 has gone live. Planner works in a similar way to WeKan; however, as the suite provides the operating system and will host many of the programmes utilised by the Force, the browser/number of user issues should be avoided or at least reduced through using this programme. That said, to ensure that the issues around functionality do not recur, the Force should look to address the recommendations raised below.

Recommendation		
We recommend that the Head of Transformation, together with the Portfolio Office, work with the IT Department responsible for the deployment of Microsoft Planner (following the roll-out of Office 365) to undertake thorough testing of the programme prior to any data transfer to ensure this works as intended and delivers the required benefits.	Priority Score	2
Agreed Action	Timescale	31 August 2020
The Force is ensuring that deployment of O365 is prioritised for T&I directorate, so that the use of MS Planner for the SDP can be established as soon as possible – ensuring the configuration / business rules / testing plan are robust enough to make the launch successful and allow the system delivers the intended benefits.	Responsible Officer	Head of IT / Head of Transformation
Recommendation		
We recommend that the Portfolio Office within the Transformation Department look to review the level of detail in the SDP to ensure that the proposed level of granularity is required, in order to potentially reduce the amount of data held which could cause system/access problems. Furthermore, the Portfolio Office should ensure that there is consistency around the use of the system and level of detail required.	Priority Score	3
Agreed Action	Timescale	30 April 2020
Portfolio Office to develop and maintain a clear set of business rules around use of the SDP to ensure its ongoing reliability, and relevance and consistency of content.	Responsible Officer	Delivery Manager - Portfolio

1.2 Finding and Action

Issue	Risk
The revised governance framework has not yet been streamlined, with a lack of control/scrutiny around the establishment of new meetings and incomplete Terms of Reference.	Meetings are inefficient, ineffective and not delivering required outcomes including satisfactory information flow and continue to place additional strain on senior leaders' time, leading to potential non-achievement of objectives around governance and desired value for money.

Findings

As per the Blueprint, the Strategic Framework sought to introduce *"a lean and proportionate governance framework to provide organisational control and assurance – supporting collaborative problem solving and decision making......A streamlined governance structure - reducing our reliance on meetings to progress activity. This is predicated by increased onus on individual and group accountability for delivery at Department and Directorate level."*

A key objective of the governance improvements under the new Strategic Framework was to improve the information flow and streamline governance between the various levels of the organization, whilst seeking to ultimately reduce the amount of time spent in meetings, particularly for senior leaders. The Blueprint clearly sets out the structure for how this will work, with a Constabulary Management Board (CMB) being the heart of the new Framework. Membership includes the Chief Constable, Deputy Chief Constable, Assistant Chief Constables, Chief Officer – Finance, Resources and Innovation and other senior management stakeholders. The CMB provides the key means to assure delivery against the objectives in the force strategies (primary authority) and the agenda will be framed around the corporate strategies. Alongside the CMB sits the Strategic Planning Meeting (SPM), which is responsible for Horizon Scanning and Strategic Planning. The purpose of the meeting is to ensure the Force understands the changing context, identifies implications, and remains on track to achieve the Force vision. Membership comprises of the Chief Constable, Deputy Chief Constable, Assistant Chief Constables, Chief Officer – Finance, Resources and Innovation and senior operational and Directorate leads

Underneath the CMB sits a range of Boards, Leadership Meetings, Permanent Support Meetings and Temporary Themed Groups. This includes Directorate Leadership Meetings (DLMs) which, from interviews with stakeholders across the organization and subsequent provision of minutes/notes, were found to be operating regularly and the interviewees felt these to be effective forums. Above the DLMs in the structure sit the Senior Leadership Meetings (SLMs) which involve the Deputy Directors of the eight Directorates across the organisation, with the Chair rotating for each meeting. From interviews with stakeholders as part of the audit, there seemed to be little benefit gained from these particular meetings and they did not serve to provide an upward flow from the individual DLMs.

Interviews with stakeholders confirmed that they felt they were still attending an inordinate number of meetings and the benefits of the streamlined governance approach were yet to be realised. It was commented upon that additional meetings were continuing to be introduced and there appeared to be little control/scrutiny around this. Whilst a cultural change regarding meetings is likely to take time, it would be beneficial for a 'gatekeeper' role to be introduced to manage this and, as such, a recommendation to this effect has been raised below.

All segments of the governance structure should have a Terms of Reference (ToR) in place, based upon a template contained within the Blueprint. This ToR has focused the requirements for each meeting to have explicit objectives and "Inputs, Processes and Outputs." Copies of the ToRs for the meetings within the governance structure were provided and it was clear that a significant proportion of these were incomplete through omissions of key information as dictated by the template within the Blueprint. Across the documents reviewed, ToRs were missing detail regarding inputs, processes and outputs, aims of the group concerned, purpose for agenda items, membership roles and responsibilities and administration requirements. As a result, we cannot provide assurance that these meetings were delivering as intended, as the objectives and other pertinent information had not been recorded.

The Head of Transformation has confirmed that a governance and portfolio structure review is underway and Chief Officer Group (COG) and the Senior Leaders across the organisation will be agreeing revised arrangements. Transition to the new arrangements is intended to start in April. This review is intended to provide an opportunity to further refine the number of meetings as well as re-clarifying and refreshing terms of reference for all meetings, business rules and delegated authorities.

Recommendation		
We recommend that the Head of Transformation oversees to completion the review of the governance structure as planned, which will map out the value of the current meetings taking place and makes changes to this as required.	Priority Score	2
Agreed Action	Timescale	30 June 2020
The governance review will be used as an opportunity to further rationalise meeting structures and arrange Force governance more intuitively, as well as refresh documentation and templates (including terms of reference) and clarify business rules (e.g. commissioning of change, delegated authorities).	Responsible Officer	Head of Transformation and Governance Manager
Recommendation		
We recommend that the Portfolio Office / Governance Secretariat with the Transformation and Improvement Directorate take on a gatekeeping role in relation to governance meetings, ensuring that Terms of Reference for all meetings are complete and accurate, whilst maintaining a scrutiny role for new meetings established in ensuring that these support the requirements and objectives of the Strategic Framework. This should drive forward a cultural change around meetings.	Priority Score	3
Agreed Action	Timescale	31 July 2020
We will consider how the governance secretariat and portfolio office within T&I, and the staff office within COG, can work together to ensure that meeting structures remain manageable and fit for purpose, and better communicate across the organisation around meeting and governance arrangements so there is common understanding and consistency.	Responsible Officer	Head of Transformation

1.3 Finding and Action	
Issue	Risk
Obligations and processes around risk management between and at the operational and strategic levels are not currently clear and are potentially over-complicated	Risks are realised as they are not effectively managed, leading to potential adverse impacts on people, reputation, finance and service delivery.
Findings	

Risk management is integral to good governance. Under the Strategic Framework, the intention is to refocus the Strategic Risk Register (SRR) to represent the key strategic risks as ‘failure to deliver the four Corporate Strategies’. Pre-existing strategic risks will be incorporated into the four risks e.g. ‘Lack of capacity and/or capability to deliver an effective policing service’ is incorporated within ‘Failure to deliver the Service Strategy’. At the time of the audit, this had not yet been achieved and the SRR remained in its existing state. The proposed changes to the risk management approach under the Strategic Framework do not align to risk management best practice, utilising a cause, event and effect approach. The logic for aligning the SRR to the four corporate strategies is clear, however these could be phrased more in line with best practice. It should also be ensured that all current risks will clearly ‘map’ to fit under the suggested risk framework. We understand that the Governance Manager was in the process of meeting with key risk owners and refreshing the SRR as we were compiling our report.

Under the Strategic Framework Blueprint, the CMB is responsible for reviewing the SRR. Upon review of the minutes of the CMB for the past six months (also confirmed by the Governance Manager), it was apparent that the SRR was not presented for the previous four months of meetings at the time of testing. This was discussed with the Head of Transformation, who confirmed that the intention is that the SRR will instead be presented to the Strategic Planning Meeting (SPM) as it was felt this forum was more strategic and had a more forward focus. As a result, review of the SRR has been quarterly rather than monthly. The ToR for the CMB requires updating accordingly (the SPM ToR details review of strategic risk as one of its responsibilities already) and a recommendation has been raised to this effect below. It is noted that core membership of the two groups is very similar, and thus the audience for the SRR will be largely the same.

The Blueprint removes the requirement for Directorate level risk registers underneath the SRR. There was disparity between the understanding of the stakeholders interviewed in terms of their responsibilities for risk management. This currently presents a gap in the risk management process and it makes the link between the Directorate/operational level risk management and the strategic risk management process unclear. Furthermore, it is not clear how Directorate risks that may not directly align to the strategies would be recorded and monitored.

Going forward, the conduit between the operational and the SRR will be the assurance framework underpinning the Single Delivery Plan (SDP). This is not, as stated above, fully operational as intended at the time of the audit. As part of the requirement for providing assurance under the SDP, the Force is using a risk-based approach. As such, the intention, as per the Blueprint, is that a ‘scrutiny score’ is derived from the risk assessment and the current assurance level associated with an activity. The ‘scrutiny’ score highlights those activities requiring most attention which should drive proportionate assurance interventions. This detail is intended to be included in the SDP, adding to the data requirements discussed above. Risk scores would then be aggregated and produce an overarching RAG status, fed by individual risk scores and would feed in to the SRR. Discussion with the Head of Transformation highlighted the complicated nature of the intended risk approach within the Blueprint and that this is currently being reviewed by the Governance Manager. The Head of Transformation has confirmed that the management of risk within the organisation was being reconsidered as part of the governance review and also the development of the refreshed single delivery plan for 2020-21. This will simplify the approach. The SRR has also been reviewed and is now much more in line with the original intention in the Blueprint (i.e. with risks associated with non-delivery of the strategies). We support this review as the risk management processes proposed appear overly complicated and are likely to struggle to drive forward the desired risk-based approach to all levels of the organisation.

Recommendation

We recommend that the Head of Transformation and Head of Improvement ensure that the review of the risk management approach gives consideration to the following areas: ▪ The cohesion between the Directorate-level management of risk and the SRR as it currently stands to ensure that there are no gaps in oversight of risk; ▪ The proposed wording of the new risks in the SRR and whether this could be aligned to best practice;	Priority Score	2

▪ Seeking to reduce complication in the management of risk through the SDP to ensure that this is accessible throughout the organisation to drive the culture of risk management; ▪ How it will be ensured that Directors, Deputy Directors and Chief Superintendents are made aware of the requirements of them in managing risk, both now and going forwards.		🟥
Agreed Action	Timescale	30 April 2020
We will review our risk processes as set out in the Blueprint and ensure a more intuitive approach that is better understood and embedded in our new Single Delivery Plan and governance arrangements.	Responsible Officer	Head of Transformation Head of Improvement Governance Manager
Recommendation		
We recommend that the Head of Transformation and Head of Improvement ensure that the Terms of Reference for the CMB is updated to reflect the amended obligations of reviewing the Strategic Risk Register.	Priority Score	3
Agreed Action	Timescale	30 June 2020
As part of the governance review, we will ensure that the terms of reference for existing meetings that will continue to exist (e.g. CMB and SLM) are reviewed so they are up to date and aligned with any new governance meetings.	Responsible Officer	Head of Transformation Head of Improvement Governance Manager

1.4 Finding and Action	
Issue	Risk
Handover plans not fully formalised for Business as Usual.	The Strategic Framework is not fully embedded into Business as Usual and the benefits are not realised.

Findings

The initial Blueprint for the Strategic Framework stated that the project was due to be closed down in July 2019 and a Post Implementation Review (PIR) was due to follow in December 2019. This has not happened as yet, primarily due to the delays with WeKan although the governance, risk and assurance mechanisms also remain to be fully embedded. The Head of Transformation confirmed that the intention is to 'close' the project down in May 2020 and then complete the PIR around December 2020. This will be dependent on the roll-out of Microsoft Planner (and indeed Office 365). It was not clear whether a formal handover plan to translate the project to Business as Usual was in train at the time of this review and this was raised by some stakeholders interviewed.

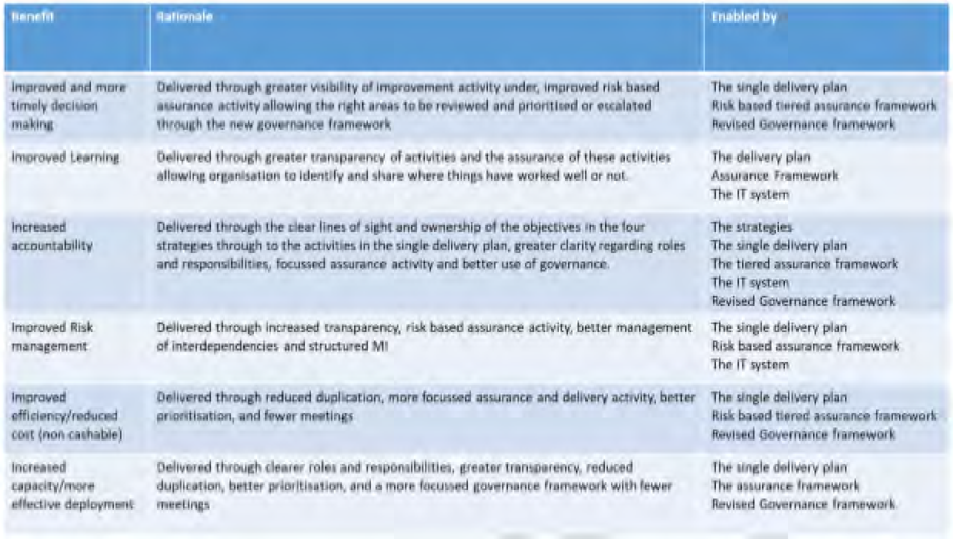
Recommendation		
We recommend that the Head of Transformation develops a formal handover plan for the closure of the project which translates into Business as Usual for the Force and that this outlines key roles and responsibilities going forward.	Priority Score	3
Agreed Action	Timescale	31 August 2020
The closure report for the SF Project to include a full handover plan outlining key roles and responsibilities going forward.	Responsible Officer	Head of Transformation

1.5 Finding and Action	
Issue	Risk

Benefits from the Strategic Framework are not SMART and may not be tangible.	Measures of benefits do not exist or cannot be quantified, increasing the risk that the project does not fully deliver maximum impact or realise the intended benefits.

Findings

The Blueprint for the Strategic Framework outlines the following benefits to be derived from its implementation and is further supported by a full benefits map in the appendices:



Benefit	Rationale	Enabled by
Improved and more timely decision making	Delivered through greater visibility of improvement activity under, improved risk based assurance activity allowing the right areas to be reviewed and priortised or escalated through the new governance framework	The single delivery plan Risk based tiered assurance framework Revised Governance framework
Improved Learning	Delivered through greater transparency of activities and the assurance of these activities allowing organisation to identify and share where things have worked well or not.	The delivery plan Assurance Framework The IT system
Increased accountability	Delivered through the clear lines of sight and ownership of the objectives in the four strategies through to the activities in the single delivery plan, greater clarity regarding roles and responsibilities, focussed assurance activity and better use of governance.	The strategies The single delivery plan The tiered assurance framework The IT system Revised Governance framework
Improved Risk management	Delivered through increased transparency, risk based assurance activity, better management of interdependencies and structured MI	The single delivery plan Risk based assurance framework The IT system
Improved efficiency/reduced cost (non cashable)	Delivered through reduced duplication, more focussed assurance and delivery activity, better prioritisation, and fewer meetings	The single delivery plan Risk based tiered assurance framework Revised Governance framework
Increased capacity/more effective deployment	Delivered through clearer roles and responsibilities, greater transparency, reduced duplication, better prioritisation, and a more focussed governance framework with fewer meetings	The single delivery plan The assurance framework Revised Governance framework

The Blueprint states that objectives should be SMART (Specific, Measurable, Agreed, Realistic and Time-bound); however, whilst these are benefits rather than objectives, the above table and benefits map referenced are not fully SMART. Whilst the aforementioned are all valid benefits, these would be strengthened through more tangibility being given to what constitutes 'Improved' for example and would support the eventual outcomes of the PIR.

Recommendation

We recommend that the Head of Transformation considers whether it would assist the delivery of the Strategic Framework to add more tangibility/quantifiable metrics to the expected benefits of the Strategic Framework, to support the PIR in gauging the success of the project.	Priority Score	3
Agreed Action	Timescale	31 August 2020
Agreed – as above	Responsible Officer	Head of Transformation

Authors and Distribution

Please note that this report has been prepared and distributed in accordance with the agreed Audit Charter and procedures. The report has been prepared for the sole use of the Partnership. No responsibility is assumed by us to any other person or organisation.

Report Authors

This report was produced and issued by:

Laura Wicks	Assistant Director
Ed Nichols	Principal Auditor

Distribution List

This report has been distributed to the following individuals:

Jennifer Grannan	Head of Transformation
Sarah Omell	Head of Improvement
Mark Simmonds	Interim Chief Executive, Avon and Somerset OPCC
Nick Adams	Chief Finance Officer, Avon and Somerset Police and Interim Chief Finance Officer, Avon and Somerset OPCC
Jane Walmsley	Inspection and Audit Co-Ordinator
Helen Graham	Improvement Services Co-Ordinator

If you require the report in an alternative format, please contact SWAP Head Office.

AVON & SOMERSET POLICE & CRIME COMMISSIONER

SWAP INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

6g

Avon and Somerset Police

Personal Issue of Assets

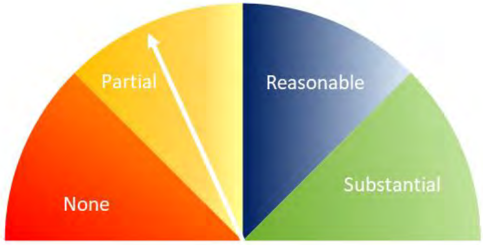
Final Report

Issue Date: 7th February 2020

Working in Partnership to Deliver Audit Excellence

Executive Summary

Audit Opinion



Partial

In relation to the areas reviewed and the controls found to be in place, some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.

Recommendation Summary

Priority	Number
Priority 1	**0**
Priority 2	**8**
Priority 3	**1**
Total	**9**

Audit Conclusion

Effectiveness of Control Framework

Due to weaknesses identified with the design and application of the current control framework for issuing, recording and managing personal assets / devices (which include mobile phones, laptop, body worn video cameras (BVWC) etc.), the assurance opinion we have been able to provide is Partial. The design and application of the current control framework exposes the Constabulary to a sufficient degree of risk of personal assets – valued at £13m in the 2018/19 Group Statement of Accounts - being lost or stolen. Furthermore, risks are presented around the data held on these devices should they be lost or stolen. Data protection e-learning training relevant to information security and the appropriate use of personal assets has only been completed by 39% of the organisation.

Design of Control Framework

A number of weaknesses were identified in the design of the controls relating to the systems and processes governing issue of personal assets:

- These are recorded within an electronic database called Assyst. A number of issues were identified in our testing which appear to result from system limitations in Assyst and / or manual input errors when recording information. The software is significantly reliant on the manual input of data which is inherently at risk of input error or omission.
- We initially identified over 950 allocated devices without an assigned user and. following further investigation, around 300 of these exceptions could be explained. However, a large number of devices remain unaccounted for. Personal assets without an assigned user will be difficult to locate and could potentially have been lost or stolen.
- Some of the gaps identified in the system may be remedied going forward by ensuring essential fields such as the user information field are made mandatory. However, no work is currently planned to resolve the historic gaps in data we identified.
- Assyst does not currently retain information relating to a leaver. Once an employee has left the organisation, their record will be removed from Assyst entirely. Employees are required to return any devices issued to them prior to leaving, with line managers also responsible for ensuring this occurs. To strengthen this process, Assyst should be updated (if possible) to retain leaver records.

- The Senior Technical Support Officer is in the early stages of investigating a more dynamic solution to manage assets in the long term. An ITAM (asset management discovery tool) for example is one of the solutions being explored. This tool will automatically populate information when a registered device and user accesses force systems allowing more dynamic / real-time management of assets.
- For new device orders, no independent checks (by a party not involved in the procurement and tagging process) is carried out to ensure personal devices requested were correctly delivered and accurately recorded within Assyst. Without independent checking, devices could potentially be lost or stolen at delivery, collection and recording stages of the process.
- The process to ensure the return of old or faulty devices has not been fully embedded.
- The arrangements for the disposal or sale of BWVCs which contain sensitive data have not yet been formalised. It should ale or disposal has yet occurred.
- Individuals allocated a personal asset (e.g. laptops, mobile phone etc.) are not currently required to sign and confirm that they have read relevant policies and procedures related to information security and appropriate use. Whilst we accept to so would be resource intensive and administratively difficult given the high number of individuals allocated a device, management ought to consider implementing this to strengthen the control framework.

Application of Control Framework

- Employees with devices that are faulty are required to log this with IT. The faulty device's record will be updated within Assyst as 'awaiting return' until it is returned. Our review identified over 300 instances where an employee had been issued a new device prior to the faulty device being returned. Whilst this is common practice, the process to ensure returns are eventually made is not formalised or robustly monitored. Therefore, the return of devices may take longer than required or may not occur and could result in devices and / or data being lost or stolen.
- Mobile phone and laptop disposals are managed through a contract with VFM Disposal Ltd (VFM). Under the contract, VFM are required to obtain signatures to confirm disposals / sales have occurred and supply the Constabulary with data deletion certificates for each device disposed or sold. Disposals undertaken in November 2019 were selected for review as part of this audit. No third-party confirmation from the contractor to verify that disposal / sale had actually occurred was available for review (e.g. a signature or data deletion certificates).

Audit Assessment of Agreed Themes

Theme	RAG Rating	Reason for RAG Rating
Leadership & Culture	🟧	The Senior Technical Support Officer responsible for asset management has been in post since late summer 2019. They are working to resolve historic issues in relation to asset management and are in the process of implementing controls to strengthen this area moving forward, including training on Assyst to staff in order to help ensure accuracy of record keeping; implementing cycle counts to improve accuracy of information; and exploring alternative asset management solutions. Due to the recent appointment to the role, we could only provide an amber rating.
Learning	🟧	Training is currently being delivered to staff by the Senior Technical Support Officer in order to help ensure the accuracy of record keeping within Assyst. The effectiveness of the training cannot yet be assessed. This has impacted on the rating we have been able to provide.
Diversity and Inclusion	Not Assessed	We have been unable to provide an opinion on diversity and inclusion specific to asset management processes reviewed.

Background

Personal assets / devices include the following:

- Blackberry Enterprise Service Device (various makes and models of mobile phones);
- Laptops and tablets (various makes and models);
- MiFi (4G dongles); and
- Body Worn Video Camera (BWVC).

The allocation of personal assets is governed through a 'Fixed, Agile and Deployable' (FAD) status assigned to police staff and officer following a Digital Mobilisation Programme concluded in early 2019. The Digital Mobilisation Programme sought to provide more technology to more users for a range of benefits associated with agile working and now 65% of the organisation are allocated one or more personal assets / devices (e.g. a mobile phone, laptop or both).

Corporate Risk Assessment

Audit Objective

To provide assurance that the Constabulary's internal controls in relation to the issue, management and disposal of personal assets to police officers and staff such as mobile phones, laptops and other equipment are operating effectively.

Risk	Inherent Risk Assessment	Manager's Initial Assessment	Auditor's Assessment
Personal assets are not issued, managed or disposed of properly which could result in financial loss and reputational damage.	**High**	**Medium**	**High**

Scope

The audit sought to review / consider the following:

- The arrangements in place for the issue and management of personal assets including policies, guidance and training in place for employees who are issued with a personal asset (e.g. mobile phone, laptop etc.);
- The controls in place to ensure personal assets issued are returned once the owner leaves or no longer requires them (see Sections 1.2 and 1.3 below);
- The procedures in place to ensure appropriate write off and disposal of personal assets (see Section 1.4 below); and
- How personal assets have been reflected within the accounts. The accuracy of the figures reflected were not verified as part of this review.

Findings and Outcomes

1. Personal assets are not issued, managed or disposed of properly which could result in financial loss and reputational damage.	High

1.1 Finding and Action

Issue	Risk
Essential information in relation to personal assets is not being captured within Assyst, including the details of users who have been allocated devices.	Personal assets and / or data may be lost or stolen resulting in financial loss and reputational damage to the Constabulary.

Findings

Reports of all personal assets recorded within Assyst were provided for review. Both personal assets that have been allocated to individuals and those still in stock (to be allocated) were reviewed. The data within the reports from Assyst was analysed and a number of gaps in data were identified as part of this analysis. This included missing user information for devices that have been allocated to someone and missing serial numbers for certain devices. A summary has been provided below:

Table A: Number of 'Blank' Records for Allocated (Live) Personal Assets

Field Name	BES Devices (Mobile Phones)	Laptops	Tablets	MiFI (4G Dongle)	BWVC	Total
Username	105	326	186	-	342	**959**
Serial Number	331	2	34	-	-	**367**

Table B: Number of 'Blank' Record for Unallocated (Stock) Personal Assets

Field Name	BES Devices (Mobile Phones)	Laptops	Tablets	MiFI (4G Dongle)	BWVC	Total
Username*	244	126	22	-	179	**571**
Serial Number	4	2	1	-	-	**7**

**Whilst no username has been recorded against 571 records, this is not unusual as the devices are unallocated (stock) and therefore, will not have an assigned user to them. The username fields that were found not to be blank have 'RETURNED recorded' against them.*

The gaps in data were discussed with the Senior Technical Support Officer who explained that these were a result of manual input errors i.e. when a device has been allocated, the individual responsible for updating Assyst has not completed the record properly. Therefore, this has resulted in no users being assigned to an allocated device or serial numbers for devices being updated.

There are some exceptions where a user may not necessarily be assigned. For example, 36 out of the 326 laptops without a user assigned were found to be training laptops allocated to the training school. However, the other 290 could not be accounted for. In addition, 300 out of the 342 BWVC were found to be 'pool' cameras where a police officer will collect a BWVC before commencing a tour and return it after they finish. There are still 42 BWVC which are unaccounted for. Therefore, without user information being assigned to a device, there is a risk that these devices may have been lost or stolen. No work is currently planned to resolve these gaps. We acknowledge that to do so would require a significant degree of time and resource and the value of undertaking such a project should be ascertained with input from the Chief Finance Officer to ensure assets are correctly represented in the accounts.

The Senior Technical Support Officer (who has been in post for a few months) notes the above exceptions are a result of historic issues and is currently in the process of improving controls going forward to help manage this. For example, Assyst can be used to log the movement of devices through users and statuses (e.g. live, in repair, damaged. returned etc.). This essentially works as an audit trail to track a devices history / life cycle which has not been fully utilised before. Staff responsible for updating Assyst are currently being trained on using this field going forward.

The issues identified above are a result of limitations in the current asset management software (Assyst). The software significantly relies on the manual input of data which is inherently at risk of input error or omission. Some of the gaps identified may be remedied going forward by ensuring fields such as 'username', 'serial number' and 'movement' are made mandatory.

The Senior Technical Support Officer is in the early stages of investigating a more dynamic solution to manage assets in the long term. An ITAM (asset management discovery tool) for example is one of these solutions. This tool automatically would populate information when a registered device and user accesses the force system allowing more dynamic / real-time management of assets.

1.1a	Recommendation		
We recommend that the Director of Information Technology assesses whether the gaps in records within Assyst should be fully investigated and resolved and liaises with the Chief Finance Officer to ascertain the potential impact on the Constabulary and Group accounts.		Priority Score	2
Agreed Action		Timescale	31/01/2020
Agreed. Assets and users will be identified and a reconciliation performed.		Responsible Officer	Senior Technical Support Officer
1.1b	Recommendation		
We recommend that the Director of Information Technology updates Assyst to ensure that the following fields are made mandatory: ▪ Username ▪ Serial Number ▪ Movement ▪ Purchase Order		Priority Score	2

Agreed Action	Timescale	31/01/2020
Agreed. Assyst will be updated to include mandatory fields.	Responsible Officer	Senior Technical Support Officer

1.1c	Recommendation

We recommend that the Director of Information Technology, together with relevant stakeholders, review the weaknesses of Assyst as outlined within this report in order to ascertain the Constabulary's appetite to continue using Assyst as their asset management tool. This should include an assessment of the potential benefits of other, asset management solutions available on the market.	Priority Score	2
Agreed Action	Timescale	29/02/2020
Agreed. We will investigate a more dynamic solution to manage assets in the long term and a proposal will be drafted for review by the Directorate Leadership Team.	Responsible Officer	Head of IT Technical and IT Projects

1.2	Finding and Action

Issue	Risk
The process to ensure the return of old or faulty devices is not fully embedded.	Devices may not be returned, lost or stolen resulting in financial loss and reputational damage to the Constabulary.

Findings

Duplicate records within Assyst by username were identified as part of our review. These have been outlined within the table below:

Table A: Number of Duplicate Records by 'Username' for Allocated (Live) Personal Assets:

BES Devices (Mobile Phones)	Laptops	Tablets	MiFI (4G Dongle)	BWVC	Total
71	528	-	7	-	**606**

The table above highlights instances where a single user has been assigned two or more of the same device (e.g. a mobile phone) but with different asset tags and serial numbers. The total number will actually be half of the total (303), or less than half because the analysis used will have counted the same user twice against two or more devices.

A sample of duplicates were found to be a result of users being allocated a new device without their old device being returned. For example, in instances where a device is faulty and a replacement has been issued in advance of the return of the faulty item, this will result in a duplicate record within Assyst. Users with faulty devices are required to log this with IT who will update the record in Assyst as 'awaiting return' until receipt. Staff in the EUS Team responsible for ensuring the

return of faulty devices will usually allow a month before chasing officers. The process is not currently formalised or robustly monitored and therefore, the return of devices may take longer than required or may not occur.		
1.2a Recommendation		
We recommend that the Director of Information Technology implements a formal procedure which ensures all staff issued with a new replacement device return their old devices in a timely manner, considering whether it would be appropriate to request return prior to new devices being issued.	Priority Score	2
Agreed Action	Timescale	31/01/2020
Agreed. The procedure for the return of old or faulty devices will be updated / amended. The process will be embedded to ensure all relevant parties are in agreement and aware of their duties.	Responsible Officer	Senior Technical Support Officer

1.3	Finding and Action
Issue	Risk
Leaver information is not retained within Assyst.	Devices allocated to employees who have left may be lost or stolen resulting in financial loss or reputational damage to the Constabulary.
Findings	
As part of the agreed scope of the audit, we sought to review a sample of leavers who had been allocated with a personal device in order to ensure that this had been returned. Assyst does not retain information relating to a leaver and we were unable to ascertain the reasons behind this with relevant officers. Therefore, it was not possible to trace a leaver within Assyst back to the devices they have allocated. When an employee leaves the organisation, the leaver or their line manager is responsible for ensuring the return of any devices issued. The current returns process for a leaver is therefore heavily reliant on the employee or line manager returning any devices issued. It is our opinion that Assyst should be updated (if possible) to retain leaver records. Leaver information could then be used by the EUS Team to perform sample testing on a periodic basis to ensure any devices issued to someone that has left the organisation have actually been returned. This will help strengthen controls in this area.	

1.3a Recommendation		
We recommend that the Director of Information Technology investigates whether it is possible to retain information relating to someone that has left the organisation within Assyst. If possible, periodic dip sampling of leavers should occur to ensure that devices issued to them have been returned.	Priority Score	2
Agreed Action	Timescale	31/01/2020

Agreed. We will Investigate whether it is possible to retain information relating to someone that has left the organisation within Assyst (subject to compliance with retention schedules). If possible, periodic dip sampling of leavers should occur to ensure that devices issued to them have been returned.	Responsible Officer	Senior Technical Support Officer

1.4	Finding and Action

Issue	Risk
Lack of retention of documentation surrounding disposal or sale of assets and deletion of data.	Personal assets may not be properly disposed of resulting in financial loss and reputational damage to the Constabulary.

Findings

The disposal of laptops and mobile phones is managed through a contractual arrangement with VFM Disposal Ltd (VFM). Under the terms of the contract, VFM is required to obtain signatures from the Constabulary to confirm any personal assets collected by them for disposal or sale has occurred. In addition, VFM is required to provide a data deletion certificate for all assets sold or disposed. Where devices are to be disposed of or sold, the EUS Team will prepare a spreadsheet which details all assets to be collected by VFM. Usually only one EUS Team member will be present during the collection. A spreadsheet is completed detailing the asset number, serial number, make, model and type of device being disposed / sold. The completed spreadsheet is then sent to VFM and Finance and VFM will produce an invoice to be paid by Finance.

As part of this audit, we sought to review a number of disposals that have recently taken place in order to ensure that these have been undertaken in line with agreed processes and were provided with a spreadsheet detailing disposals that had occurred in November 2019. Whilst we could evidence devices had been recorded on the spreadsheet, no third-party confirmation from the contractor to verify that disposal / sale had actually occurred was available for review (e.g. a signature or data deletion certificates). This was queried with Finance who confirmed that data deletion certificates had been provided at the time of disposal. However, these had been reviewed and checked by an officer who has recently passed away but could not be provided. Copies were available from the contractor if required. Whilst we appreciate that this is an exceptional circumstance, evidence to support disposals / sales should retained going forward.

In addition to the above, there is currently no formalised process or arrangement for the disposal or sale of BWVC. The Senior Technical Support Officer explained that the Constabulary has not yet undertaken any disposals of BWVC. However, if a BWVC is faulty, these will be sent back to the supplier for repair or replacement. Due to the sensitivity of the data collected and retained on BWVC, these arrangements should be formalised at the earliest opportunity.

1.4a	Recommendation	
We recommend that the Director of Information Technology ensures signatures and data deletion certificates are obtained for any personal assets disposed of or sold. On receipt of the data deletion certificates from the contractor, the Director of Information Technology should also ensure a reconciliation is performed between the certificates provided and the assets recorded as disposed or sold to confirm all are accounted for. All records to support disposal and sale should be retained and accessible.	Priority Score	2

Agreed Action	Timescale	31/01/2020
Agreed. We will ensure signatures and data deletion certificates are obtained for any personal assets disposed of or sold. A reconciliation will be performed between the certificates provided and the assets recorded as disposed or sold to ensure all are accounted for.	Responsible Officer	Head of Procurement
1.4b Recommendation		
We recommend that the Director of Information Technology ensures a formal procedure for the disposal of BWVC is implemented.	Priority Score	2
Agreed Action	Timescale	Complete
Agreed. A process is already embedded.	Responsible Officer	Senior Technical Support Officer

1.5	Finding and Action

Issue	Risk
E-learning training which covers information relating to key principles of data protection relevant to information security and the appropriate use of personal assets may not be completed to a satisfactory level by police officers and staff.	The Constabulary may be exposed to a greater risk of breaching GDPR which could result in a substantial fine, reputational damage and negative consequences for data subjects.

Findings
E-learning training in relation to data protection explains how to handle, record and share information and it incorporates changes introduced by the GDPR and Law Enforcement Directive (LED), all of which are enshrined in domestic legislation within the Data Protection Act 2018 (DPA). The programme consists of two courses - one consists of learning content and the other contains a set of scenario-based questions. Police staff and officers are only required to complete one or the other depending on whether they have an 'operational' role or 'non-operational' role. The training is relevant to employees who have been allocated personal assets (e.g. mobile phones or laptops) specifically around information security and appropriate use of assets and information. Completion of the e-learning modules as of early December 2019 were provided. A total of 2442 police officers and staff have completed the training, which equates to 39% of the 6200 total police officers and staff (including PSCOs and volunteers (Specials etc.). It should be noted that 65% of the organisation has been issued with at least one personal asset.

1.5a Recommendation		
We recommend that the Director of Information Technology, together with the Learning Department ensures that all police staff and officers complete the data protection e-learning training. In addition to this, a process should be implemented to ensure completion rates are monitored and managed going forward. This should include performance reporting to a strategic board (e.g. the Constabulary Management Board).	Priority Score	2

Agreed Action	Timescale	Ongoing
Agreed. An email from the Data Protection Officer to Senior Leaders was sent on the 3rd January 2020 and this was also noted in the Forcewide "good to know" on the 9th January 2020. This will be reported at the next Strategic Information Management Board meeting on 11th February 2020.	Responsible Officer	Data Protection Officer

1.6	Finding and Action

Issue	Risk
No independent checks are undertaken to ensure personal devices requested were correctly delivered and accurately recorded within Assyst.	Personal assets may be lost or stolen resulting in financial loss and reputational damage to the Constabulary.

Findings
As part of the agreed scope of this audit, we sought to review devices that had been purchased in order to ensure an accurate audit trail existed between the initial purchase requisition and delivery. The intention was to cross check supporting evidence / documentation throughout the procure to pay process to ensure the items requested were in fact delivered. Assyst includes a 'purchase order' (PO) field for all devices, which should be used to record the specific PO number a device was purchased under. However, this was found not to have been used. Therefore, it was not possible to trace a sample of devices back to a specific purchase order or requisition nor from requisitions forward to records within Assyst. This is because once a device is tagged and recorded, there is currently no other field within Assyst to identify which requisition or purchase order a specific device relates to. A recommendation has been raised within Section 1.1 above to make the purchase order field a mandatory going forward. The inclusion of an independent check on all devices delivered back to requisitions should be undertaken to ensure the correct devices and quantity have been delivered. If possible, this should be undertaken by a party separate from the procure to pay process.

1.6a Recommendation		
We recommend that the Director of Information Technology considers introducing an independent check on all new devices delivered and recorded within Assyst back to supporting documentation. This should be performed by a party independent of the current procure to pay process in order to ensure devices requested were correctly delivered and recorded within Assyst. This could be undertaken by cross checking PO numbers allocated against devices within Assyst back to supporting purchasing documentation.	Priority Score	3
Agreed Action	Timescale	31/01/2020
Agreed. A cross check of PO numbers allocated against devices within Assyst back to supporting purchasing documentation will be performed.	Responsible Officer	Senior Technical Support Officer

1.7	Finding
Cycle counts / checks to ensure devices within Assyst are still Constabulary's possession were found not be undertaken at the time of the audit. However, these are planned to be conducted in the new year. A tool has been developed by the Senior Technical Support Officer which will cross check a devices asset tag back to Assyst to ensure firstly that the device has been recorded within Assyst and secondly, the information against the device is accurate. These checks will help ensure records are accurate. As a result of the planned implementation cycle counts / checks, no formal recommendation will be raised around this area. The information has been included for management consideration.	

Authors and Distribution

Please note that this report has been prepared and distributed in accordance with the agreed Audit Charter and procedures. The report has been prepared for the sole use of the Partnership. No responsibility is assumed by us to any other person or organisation.

Report Authors

This report was produced and issued by:

Laura Wicks	Assistant Director
Juber Rahman	Senior Auditor

Distribution List

This report has been distributed to the following individuals:

Nick Lilley	Director of Information Technology
John Smith	Chief Executive, OPCC
Mark Simmonds	Chief Finance Officer, OPCC
Nick Adams	Chief Finance Officer, Avon and Somerset Constabulary
Jane Walmsley	Inspection and Audit Co-Ordinator

6h

Avon & Somerset Constabulary and Office of the Police and Crime Commissioner Joint Audit Committee (JAC)

Report of Internal Audit Activity- March 2020

Internal Audit ▪ Risk ▪ Special Investigations ▪ Consultancy

Unrestricted

Executive Summary

The Assistant Director is required to provide an annual opinion to support the Annual Governance Statement.

As part of our plan progress reports, we will look to provide an ongoing opinion to support the end of year annual opinion.

We will also provide details of any significant risks that we have identified in our work.

We have sought to make our Committee Papers more concise and as such, we will formally report on our performance once a year. To support this, we have included a reminder of our assurance opinions and risk assessment in Appendix B, to avoid duplication in each report presented.

The Chief Executive for SWAP reports company performance on a regular basis to the SWAP Directors and Owners Boards.

Audit Opinion and Summary of Significant Risks

Audit Opinion:

The majority of finalised reports issued in the year to date have been provided a Partial assurance opinion. This suggests that some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives. We have discussed the provision of our Draft Annual Internal Audit Opinion with the Chief Finance Officer and will look to provide this in mid-May, to allow for inclusion with the Draft Annual Governance Statement in the Statement of Accounts. In completing our Opinion, we will make reference to the assurance work undertaken during the year, together with the regional work and work of any other assurance providers where necessary and coverage afforded to internal controls.

Progress of 2019/20 Internal Audit Plan

At the time of reporting, the majority of audits scheduled for Quarters 1-4 have been completed or reached report stage. There are some brief reports around Income Generation (part of the Accounts Payable audit) and Follow Up of previous recommendations remaining to be completed. Copies of the following reports are submitted with this Quarterly Update:

- Cyber Security;
- Refreshing the Strategic Framework;
- Fleet Management;
- Data Quality Training; and
- IT Business Continuity.

The Personal Issue of Assets (Final report for noting) is also provided for reference. Members received the Draft report at the January JAC Meeting.Further detail is provided in Appendix A and is summarised in the table below:

Performance Measure	Performance
Delivery of Annual Audit Plan	
Completed	83%
Work at Report Stage	0%
Fieldwork/In Progress	17%
Scoping / Not Yet Started	0%

Unrestricted

Significant Risks:

The following recommendation from the IT Business Continuity audit has been assessed as a significant corporate risk:

- Over reliance on the IT service to maintain Corporate business continuity resulting in a loss of organisation wide service continuity in the event of a disruption to IT services.

Follow up of Recommendations:

As agreed, we have followed up on the implementation of relevant recommendations raised by the previous auditors on Key Financial Controls and Chief Constable & PCC Expenses during the course of our own work in these areas. Other outstanding recommendations from previous audits are in the process of being followed up at the time of writing. It is worth noting that this work is being carried out to complement the internal follow up processes of the Audit and Inspection Team, on which we have placed reliance as considered appropriate.

Regional Audit Work

We have completed a piece of benchmarking work considering the sources of assurance which feed into the Annual Governance Statement (AGS), copies of which have been provided to the regional Directors of Finance. Fieldwork was ongoing at the time of writing for the Fleet benchmarking review and the Forensics Performance and Tasking.

Internal Audit Plan Progress 2019/20 Appendix A

Link to FMS	Audit Area	Period	Audit Days	Status	Opinion	No of Recs	1 = Major	↔	3 = Minor
							Recommendation		
							1	2	3
Force Functions	Workforce Plan	Q2	15	Completed	Partial	3	-	1	2
Finance	Payroll & Expenses	Q3	15	Completed	Reasonable	4	-	1	3
Finance	Overtime Payments	Q3	15	Completed	Partial	3	-	2	1
Finance	Accounts Payable (Part of Key Financial Controls)	Q3	15	Completed	Partial	6	-	3	3
Finance	Personal Issue of Assets	Q3	15	Completed	Partial	9	-	8	1
IT & Information Management	IT Cyber Security	Q3	15	Completed	Advisory	N/A	-	-	-
Governance, Fraud and Risk Management	Refreshing Strategic Framework	Q4	15	Completed	Partial	8	-	3	5
Force Functions	Fleet Management	Q4	15	Completed	Partial	9	-	8	1
IT & Information Management	IT Business Continuity	Q4	15	Completed	Partial	4	-	4	-
IT & Information Management	Data Quality	Q4	15	Completed	Partial	5	-	5	-
Governance, Fraud and Risk Management	Contribution to Regional Police Audit Work	Throughout Year	5	In Progress	-	-	-	-	-
Governance, Fraud and Risk Management	Follow Up	Throughout Year	5	In Progress	-	-	-	-	-

**A supplemental piece of comparison work regarding Income Generation across the regional Forces remains to be completed and will be reported on separately*

.

Unrestricted

Audit Framework and Definitions — Appendix B

Assurance Definitions

None	The areas reviewed were found to be inadequately controlled. Risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
Partial	In relation to the areas reviewed and the controls found to be in place, some key risks are not well managed and systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
Reasonable	Most of the areas reviewed were found to be adequately controlled. Generally, risks are well managed but some systems require the introduction or improvement of internal controls to ensure the achievement of objectives.
Substantial	The areas reviewed were found to be adequately controlled. Internal controls are in place and operating effectively and risks against the achievement of objectives are well managed.

Definition of Corporate Risks

Risk	Reporting Implications
High	Issues that we consider need to be brought to the attention of both senior management and the Audit Committee.
Medium	Issues which should be addressed by management in their areas of responsibility.
Low	Issues of a minor nature or best practice where some improvement can be made.

Categorisation of Recommendations

In addition to the corporate risk assessment it is important that management know how important the recommendation is to their service. Each recommendation has been given a priority rating at service level with the following definitions:

Priority 1	Findings that are fundamental to the integrity of the service's business processes and require the immediate attention of management.
Priority 2	Important findings that need to be resolved by management.
Priority 3	Finding that requires attention.

SWAP work is completed to comply with the International Professional Practices Framework of the Institute of Internal Auditors further guided by interpretation provided by the Public Sector Internal Audit Standards (PSIAS) and the CIPFA Local Government Application Note.

MEETING: **Joint Audit Committee**	DATE: **19th March 2020**	AGENDA NO: **8**
DEPARTMENT: **OPCC**	AUTHOR: **Ben Valentine**	
NAME OF PAPER: **OPCC Summary of Strategic Risk Management**	PURPOSE: **Information**	**OPEN SESSION**

1. PURPOSE OF REPORT AND BACKGROUND

This report provides members of the Joint Audit Committee (JAC) with an overview of any significant changes to the Office of the Police and Crime Commissioner (OPCC) Strategic Risk Register (SRR), and other points related to the management of risk, in the period of time since the last JAC meeting held on 16th January 2019.

2. POINTS OF NOTE

There have been no changes to the assessment of any of the risks on the SRR since last reported to the JAC.

Covid-19 (Novel Coronavirus)

At the time of writing the UK remains at the containment stage of response. Although the Government has acknowledged the virus will spread in a significant way and anticipate that 20% of the workforce could be off work at any one time.

Additional demand may also arise from public order incidents and the potential need to enforce emergency measures, if put in place.

With these two factors combined the service the police can deliver is going to be restricted. The impact will not be limited to policing; other partners, criminal justice agencies and victim support services will also suffer reduced levels of service. All of these factors will impact on delivery of the Police and Crime Plan (SR2).

A further strategic impact will be the ability to deliver the officer uplift. This will likely affect availability of candidates, the ability to process them through the assessment and application process and – if educational establishments are some of the first to be closed – this will delay their onward training and could postpone them becoming operationally competent. Although the initial on-boarding of candidates will be a problem suffered nationally the particular risk around educational establishments will be unique to those forces that have converted to the Police Constable Degree Apprenticeship.

The OPCC is following Government advice and is liaising closely with the Constabulary to work in a consistent manner. Although recognising the Constabulary need to take greater levels of precaution because of the critical nature of their work.

The OPCC is ensuring its contingency plans are up to date and also moving to a position of attending meetings remotely where possible and accepting that staff may be working from home more. The office is also considering how it continues to fulfil its statutory duties (like Independent Custody Visitors) whilst ensuring the welfare of the volunteers who do this.

The other significant effect Covid-19 – and the Government response to this – could have is to delay the Police and Crime Commissioner elections. There has not been any official message to plan for this yet but considering the Government response is to delay the peak of the outbreak to May this has to be considered a possibility. However if this were to happen the current PCC will remain in office until the elections.

This is the only significant factor that has changed on the SRR; how this effects the assessment of the risks will be discussed at the OPCC Management Board on 12th March 2020.

AVON & SOMERSET
POLICE & CRIME
COMMISSIONER

Office of the Police and Crime Commissioner for Avon and Somerset

Strategic Risk Register

March 2020

A Strategic Risk is anything that might impede the delivery of the organisational objectives. Risk management is the process by which these risks are identified, assessed and controlled. This risk register is the document which records these risks and related information.

Risk is assessed by considering the causes of the risk and the consequences if that risk were to happen. The scoring is therefore based on the likelihood multiplied by the impact. The below grids explain the scoring in more detail. Risk is about planning for the future so when considering the assessment it goes beyond current performance.

Impact	5 Extreme	5	10	15	20	25
	4 High	4	8	12	16	20
	3 Moderate	3	6	9	12	15
	2 Low	2	4	6	8	10
	1 Negligible	1	2	3	4	5
		1 Rare	2 Unlikely	3 Possible	4 Likely	5 Almost Certain
		Probability				

Probability	
5 Almost Certain	Likely to occur within a twelve-month time period, or about a 75% probability of occurrence
4 Likely	Likely to occur within a two-year time period, or about a 50% probability of occurrence
3 Possible	Likely to occur within a three-year time period, or about a 25% probability of occurrence
2 Unlikely	Likely to occur within a five-year time period, or about a 15% probability of occurrence
1 Rare	Likely to occur in a ten year period, or about a 5% probability of occurrence

Impact	
5 Extreme	• Fatality of any individual • Financial impact greater than £1/2 m • Vote of no confidence from Local Authorities - failed • National media attention • Government/ HO intervention • Total disruption to service • Exceptional/long term reputational damage
4 High	• Serious life-threatening injury of any individual • Financial impact greater than £1/4 m • Vote of no confidence from Local Authorities - failed • Regional media attention • Adverse comment by Minister / auditor • Major service disruption/reputational damage
3 Moderate	• Serious non-life-threatening injury of any individual • Financial impact greater than £100k • Criticism from the Police and Crime Panel • Local media attention • Significant service disruption • Significant reputational damage
2 Low	• Minor injury of any individual • Financial impact up to around £100k • Multiple thematic complaints • Some service disruption • Some negative consequences relating to reputation
1 Negligible	• Slight injury of any individual • Low level financial loss • Isolated complaints • Minor service disruption • Minor/contained negative consequences

The unmitigated scores are the assessment based on the current position with no action taken or controls in place. The mitigated scores are based on the success of the controls (anticipated or actual) in reducing the risk.

It should be noted that the OPCC and the Constabulary are separate organisations and therefore each may assess the same risk as being at a different level. This is most evident in the risk of failure to deliver the police and crime plan. This exists on both Strategic Risk Registers but may score differently. One of the main reasons for this is that the OPCC assess delivery of the plan as a whole which relies on agencies, other than the Constabulary to fully deliver e.g. the CPS and Courts. Whereas when the Constabulary assess this risk they need only consider the parts of the plan they are expected to deliver. A difference may also be caused whether considering the risk in the short, medium or long term.

RISK			ASSESSMENT		
Risk	URN	Owner	Unmitigated Probability	Unmitigated Impact	Unmitigated Risk
Governance Failure	SR1	CEO	5	4	20
			Mitigated Probability	Mitigated Impact	Mitigated Risk
			4	4	**16**
			Mitigated Risk change:		◄►

Cause	Impact
● Long term CEO has left ● The same person cannot discharge the role of Monitoring Officer and s151 duties of the CFO ● Failure to deliver OPCC statutory requirements: - Police & Crime Plan and priorities (SR10) - Policing Precept budget - Community safety, victims services and other partnership outcomes effectively (SR9) - Hold the Chief Constable to account - Address conduct or performance of Chief Constable - Oversight of complaints against Chief Constable - Custody Visiting Scheme ● Ineffective scrutiny and oversight of services and outcomes delivered by the Constabulary including delivery of the Strategic Policing Requirement ● Ineffective arrangements for complaints and serious cases ● Failure to ensure adequate transparency of the OPCC and/or the Constabulary ● Failure to ensure effective risk management and support the delivery of service ● Failure to ensure Chief Constable sets appropriate culture, ethics and values ● Lack of control/influence over other Criminal Justice agencies ● National appetite for PCCs portfolio to extend to Fire & Rescue Services after next elections – taking on any new responsibilities as there are more likely to be governance failures whilst the team learn.	● Failure to deliver the Police & Crime Plan (SR2) ● Financial loss (SR3) ● Damaged reputation and reduced public confidence (SR5) ● Damaged relationship with Constabulary, commissioned services or partners ● Government criticism or penalties ● Panel criticism ● Sub-standard performance results and poor inspection outcomes ● Force not efficient/effective ● Risks not managed ● Failure to improve the delivery of the broader Criminal Justice Service

MITIGATION			
Controls	Review date	Owner	Commentary / Controls updates
● OPCC Management Board (OMB) - allows greater oversight of performance, risks and issues and provides a formal decision making mechanism for non-Constabulary business.	June 2020	PCC/CEO	● OMB established Feb 2020 and will be a monthly meeting.
● Current OPCC CFO acting as interim CEO and Monitoring Officer	June 2020	PCC/CEO	● Although the s151 officer for the PCC will not be independent of the Constabulary the interim CEO has the knowledge and experience to advise the PCC on financial matters helping maintain checks and balances.
● During the interim period the CFO s151 duties of the OPCC will be undertaken by the Constabulary s151	June 2020	PCC/CEO	
● Police and Crime Board (PCB)		CEO	● PCB is monthly following CMB and continues to be the principal joint decision making forum and provides the PCC formal oversight of the Constabulary.
● PCC and Chief Constable 1:1s		PCC	
● OPCC attend Constabulary Management Board and other strategic meetings (open invitation from the CC).		CEO	● The internal audit report on governance concluded that the PCC and CC have an adequate and effective framework for risk management, governance and internal control.
● Audit Committee, audit, annual governance statement		CFO	
● Police and Crime Panel meetings		PCC	
● COG attendance at weekly OPCC SLT		CEO	● CoPaCC transparency award received.
● Force Management Statements		SPPO	● OPCC Plans developed with work streams that detail activity covering all statutory requirements and OPCC team appointed owners to statutory duties.
● Police and Crime Plan Annual Report		SPPO	
● Victim Services appointed and managed by the OPCC Commissioning Team		Head of C&P	
● Scheme of governance and Governance Boards	June 2020	CFO	
● Scrutiny of complaints through the Independent Residents Panel		Volunteer Manager	
● SLT lead and increased dedicated capacity to deal with complaints and conduct and appeals		Head of C&C	
● Transparency Checklist		Office Manager	
● The Constabulary Strategic Framework has revised the Mission Vision and Values and delivery and governance arrangements (which will allow greater oversight of risk and assurance by the OPCC)		SPPO	● Constabulary Mission Vision Values continues to be embedded but not all elements of the Strategic Framework are fully developed. Since being live there has been a governance failing in relation to Lighthouse.
● Working with Joint DPO to ensure good information governance and compliance with GDPR and DPA 2018.		Office Manager/ SPPO	

Risk	URN	Owner	Unmitigated Probability	Unmitigated Impact	Unmitigated Risk
Failure to deliver the Police and Crime Plan	SR2	CEO	5	4	20
			Mitigated Probability	Mitigated Impact	Mitigated Risk
			4	4	**16**
			Mitigated Risk change:		◄►

Cause	Impact
● Covid-19 (novel coronavirus) – up to a fifth of the workforce could be off at any one time based on current estimates. This could have a severe on the ability to police and will mean a reduction in service. If Covid19 reaches an epidemic it may also mean additional demand, e.g. increase public order incidents, at a time when resource levels are low. This would likely affect the ability to meet police officer recruitment targets. Will impact the ability of commissioned services to support victims. ● Response timeliness ● Poor data quality ● Positive Outcomes - not seeing the improvements hoped for - particularly of Op Remedy crimes. ● Uncertainty of delivery following Neighbourhoods review - yet to see improvements. ● Lack of capacity/capability within the Constabulary (see Constabulary SRR commentary) - Investigations vacancies critical ● Lack of representation in the Constabulary workforce ● National rape crisis reduces confidence in the entire Criminal Justice System ● Lack of control/influence over other Criminal Justice agencies ● Government may want a more centralised/national approach to policing – the key outcomes measures scrutinised may differ from the local approach and split the focus of policing. ● Increased numbers of officers will result in more people going through the Criminal Justice System – unknown if other agencies will be funded to deal with the increased volume – particularly a concern in terms of prisons and probation. ● ORI01 – Not all VIP victims correctly referred to Lighthouse ● ORI08 – Lighthouse failing to meet SLAs about victim contact ● ORI14 – Lack of response trained drivers ● ORI15 – Increased demand on Patrol officers	● Loss of legitimacy in the OPCC and Constabulary ● Loss of public confidence/trust in the OPCC (SR4) and Constabulary ● Failure to keep people safe ● Failure to protect and support vulnerable people ● Failure to bring offenders to justice ● People will feel unsafe ● Police and Crime Panel criticism and/or fail to agree precept increase

MITIGATION

Controls	Review date	Owner	Commentary / Controls updates
● Police and Crime Board (PCB) discusses performance, assurance and risk	June 2020	CEO	● OPCC attendance at CMB and the PCB which follows this continues to work well in terms of assurance and open dialogue about areas of concern where the plan may not be delivered.
● PCC and Chief Constable 1:1s		PCC	
● OPCC attend Constabulary Management Board and other strategic meetings (open invitation from the CC).		CEO	● The Strategic Threat Assessment and Strategic Intelligence Requirements documents raise concerns around the Constabulary's ability to deliver against the Plan, but HMICFRS inspections indicate good progress.
● Audits and Inspections (HMICFRS & SWAP) overseen by Joint Audit Committee		CFO	
● Internal assurance mechanisms are in place to evaluate delivery of the Plan's objectives		SPPO	
● Service Delivery Assurance visits led by OPCC check and test for areas to improve	June 2020	SPPO	● Due to lack of capacity SDAs are conducted infrequently
● Joint performance framework allows better oversight of delivery against the plan	Apr 2020	SPPO	● Framework now live - first reported on Q2 19/20. Will need to review in light of national outcomes being defined.
● Oversight of all strategic constabulary data through Qlik		SPPO	
● Panel Meetings		CEO	
● Contacts analysis		Head of Comms	
● Forum analysis		Head of Comms	

Risk	URN	Owner	Unmitigated Probability	Unmitigated Impact	Unmitigated Risk
Financial incapability or ineffectiveness	SR3	CFO	3	5	15
			Mitigated Probability	Mitigated Impact	Mitigated Risk
			2	4	**8**
			Mitigated Risk change:		◀▶

Cause	Impact
● Op Uplift – local share of funding confirmed for 2019/20 and 2020/21 – but uncertain thereafter. Funding for 20/21 dependant on recruiting the additional officers. ● Uncertainty around associated costs of Op Uplift e.g. increase in senior officer ranks, estates provision. ● Central funding effectively ring-fenced to deliver the additional officers as 40% of the budget is from precept this still leaves significant challenges. Budget only balanced with 5 years of 2% precept rises – this may not be supported by the Police and Crime Panel. ● Capital budget not fully funded from 2023/24 – borrowing already at prudent levels and diminishing potential for capital receipts. ● Pay awards may be agreed nationally but not funded through central grants (every 1% pay rise is approx. £2.2 million). ● Increasing pension costs for officers and staff schemes. ● National work will require local funding with no control over decision making e.g. ESMCP, NPAS, national IT. ● Uncertainty of local costs in high value areas: IT and replacement of SAP. ● Police Funding formula review for 2020. ● The end of Brexit transition period (2021) could cause an economic crisis which may lead to an emergency budget and current planned spending increases dampened. ● Failure to agree, fund or deliver a balanced and sustainable budget. ● Failure to ensure value for money in OPCC and delegated Constabulary budgets.	● Run out of money - require intervention (Governmental) ● Loss of public confidence (SR5) ● Unable to fund adequate or minimum service ● Unable to fund delivery of PCC priorities (SR2) ● Unable to afford change ● Inefficiency in use of police funds wastes money and harms reputation

MITIGATION

Controls	Review date	Owner	Commentary / Controls updates
● Medium and long term financial planning ● Regular oversight of revenue & capital budget ● Maintain adequate risk-assessed reserves ● Subject to external and internal audit both overseen by the Joint Audit Committee ● Treasury Management strategy in place outcomes reviewed by CFOs and Finance meeting ● HMICFRS efficiency inspection regime		CFO CFO CFO CFO CFO CFO	● In the short term the additional funding has facilitated the growth in enabling services to support officer uplift however from 21/22 there is still uncertainty. ● 2020 maximum precept increase agreed (£10 Band D household ~ 4.59%) higher than originally anticipated but additional 2.6% will be used for specific initiatives. ● MTFP - Revenue budget for 3 years is funded. Increases in costs (especially pay and pensions) will outstrip growth meaning £6.5m savings required in total for years 4 & 5 to balance the MTFP. ● Capital plan being reviewed - funding risk as capital receipts reduce as less assets to sell. £15m borrowing facility agreed to fund longer term assets over next 4 years. ● Reserves stable but will be consumed - forecast useable non ring fenced reserves to be £12 million by 2022 (4% of net PCC annual budget). ● Assuming the additional funding for police is delivered as planned in the short term this will create an underspend position. For the current financial year the underspend has been used to 'accelerate' a number of Constabulary plans, used on reducing re-offending work and remainder will be put into reserves to manage future risk.

Risk	URN	Owner	Unmitigated Probability	Unmitigated Impact	Unmitigated Risk
Failure to engage with the public and other stakeholders	SR4	CEO	4	3	12
			Mitigated Probability	Mitigated Impact	Mitigated Risk
			3	3	**9**
			Mitigated Risk change:		◄►

Cause	Impact
● Limited resources to support this within the OPCC ● Engagement methods do not always reach a wide audience or different communities or groups ● Lack of awareness or willingness to engage from the public	● Reputational damage to both the OPCC and Constabulary ● Loss of legitimacy in both the OPCC and Constabulary ● Lack of public confidence in or awareness of OPCC (SR5) ● Partnership relationships damaged ● Failure to understand people's priorities and issues re policing and crime and which could be biased by only hearing those individuals already proactive/engaged. ● Police and Crime Plan and delivery not aligned to public concerns and priorities (SR10 & SR2)

MITIGATION

Controls	Review date	Owner	Commentary / Controls updates
● OCC/OPCC Corp Comms joint meetings		Head of Comms	
● Attendance at Gold Groups as required		CEO	
● Oversight of Operation Remedy Communications Plan through ongoing meeting structure		Head of Comms	
● Creation of an overarching strategic approach to communications going forward to work in a more focused and smarter way that enhances business objectives and strategic priorities		Head of Comms	● PCC is developing a communications strategy which will involve closer joint working on tactical communications plans under particular workstreams. The approach includes working together from planning stage to ensure roles and responsibilities for delivery are set out from the start of a piece of work and make it clear what role each organisation plays.
● Review of communications approach and channels as part of creating a new strategy		Head of Comms	
● Creation of tactical communications plans for particular workstreams (including public engagement/events) with ownership and delivery allocated to one person who is accountable		Head of Comms	
● Redesign website and review and goal focused social media communications plan		Head of Comms	● New website being designed with Constabulary SDS team; OPCC rep engaged in sections they own. New website will launch with new PCC in May.
● Meetings with local community group leaders	June 2020	PCC	
● Increase community engagement at forums, community days and events etc	June 2020	PCC	
● Joint working on communications plans for the Five Big Ideas being implemented by the Constabulary including three tier approach to cultural sensitivity training, workforce mobilisation, creation of a new cultural intelligence hub to enhance the representative workforce programme, engagement and support of communications activity in relation to Commission of Racial Equality (CORE) in Bristol		Head of Comms	● Part of the new communications strategy is to take a different approach to drop-ins by making them a part of community events that are already taking place as opposed to independent ones set up by our office for Sue that haven't seen the level of engagement desired. We will be working to include more opportunities in our diverse communities.
● Converting Comms intern post into full time permanent role will support this	May 2020	Head of Comms	
● Revise stakeholder mapping and management	May 2020	Head of Comms	● Work agreed at P&P meeting in January. Qlik will be the technological solution to this - proof of concept will be in place by end of May.

Risk	URN	Owner	Unmitigated Probability	Unmitigated Impact	Unmitigated Risk
Lack of public confidence in or awareness of OPCC	SR5	CEO	4	3	12
			Mitigated Probability	Mitigated Impact	Mitigated Risk
			3	3	**9**
			Mitigated Risk change:		◀▶

Cause	Impact
● Failure to engage with the public and other stakeholders (SR4) ● Failure to discharge statutory duties (SR1) ● Failure to deliver the Police and Crime Plan (SR2) ● Failure to set an effective Police and Crime Plan (SR10) ● Policing failures/adverse incidents (even at an operational level) can impact on the perception of the OPCC also ● Public expectation of the role of the PCC may not be matched by available funding or powers of the PCC ● Op Remedy fails to deliver expected outcomes ● Failure of the Constabulary to deliver Op Uplift (Force Futures) or if delivered failure to improve outcomes would likely impact confidence in the OPCC due to public expectations ● National rape crisis reduces confidence in the entire Criminal Justice System ● Government may want a more centralised/national approach to policing which may undermine the legitimacy of the role of PCCs.	● Loss of legitimacy in the OPCC ● Failure to demonstrate value for money ● Could undermine the working relationship between the Constabulary and OPCC ● Low voter turnout in PCC elections ● Loss of political support for the need for PCCs

MITIGATION

Controls	Review date	Owner	Commentary / Controls updates
● Gold Groups manage critical issues of public confidence		CEO	● The OPCC has a standing invite to all Gold Groups
● Embed new strategy/ways of working within OPCC	June 2020	Head of Comms	● Strategy will need to be reviewed with new PCC.
● Establishing a calendar of regular media appearances / communications activities which will also link to national days or weeks where relevant.	June 2020	Head of Comms	● Delivery of the strategy is monitored through KPIs within individual tactical plans; this will be incorporated into OMB reporting where necessary.
● Creating, owning and delivering tactical communications plans for all relevant workstreams e.g. Op Remedy, Resolve, Strategic Priorities		Head of Comms	● In order to drive forward this work the Comms team will be replacing the existing intern role with a permanent full time post.
● Redesign website	May 2020	Head of Comms	
● Election microsite		Head of Comms	● Microsite now live - will be a developing site as new questions asked for prospective candidates.

Risk	URN	Owner	Unmitigated Probability	Unmitigated Impact	Unmitigated Risk
Lack of capacity/capability within the OPCC	SR6	Office Manager	5	4	20
			Mitigated Probability	Mitigated Impact	Mitigated Risk
			4	4	**16**
			Mitigated Risk change:		◀▶

Cause	Impact
● Covid-19 (novel coronavirus) – up to a fifth of the workforce could be off at any one time based on current estimates. This will affect the ability of this office to perform all of its functions. ● CEO is leaving in Jan 2020 – loss of organisational knowledge and new CEO may bring a significant change in leadership. ● CFO taking on interim CEO role will have a knock on effect of work passed down through the office increasing demand on a number of individuals. ● Small size of the organisation and varied specialisms also makes building resilience challenging. ● A number of single points of failure within the OPCC (can cause risk to materialise temporarily during periods of prolonged absence). ● Insufficient sharing of knowledge or work among the team reduces resilience. ● Change in legislated duties of the PCC requiring additional resource/expertise. ● There has been a period of staff turnover, although vacancies have been filled there are many 'new in service'. ● Temporary loss of Senior Commissioning and Policy Officer. ● ASC OPCC has a relatively small budget (bottom quartile) compared to other OPCCs. ● Demand too high for current resource levels. ● PCC elections May 2020 - new priorities of PCC term may require rapid learning/development of staff in new areas. ● PCC elections May 2020 - a new PCC may have different ways of working or different values that may cause staff to leave. ● National appetite for PCCs portfolio to extend to Fire & Rescue Services after next elections – this will create additional demand on this office and there will be lack of experience in dealing with this area of business.	● Increased likelihood of materialisation of all other strategic risks through delivery failure ● Delivery of work is late or not to standards of quality desired

MITIGATION

Controls	Review date	Owner	Commentary / Controls updates
● Resource planning - SLT have a monthly People & Positions meeting to help mitigate this risk	May 2020	CFO	● CFO acting as interim CEO until after PCC elections when a permanent appointment is made. ● Plan agreed between PCC and SLT of new responsibilities ways of working during the interim CEO period.
● Regular team meetings to share knowledge and resolve issues		Office Manager	● Commissioning & Partnerships have recruited a new Support Officer in Dec 19 and new Support Assistant in Jan 20.
● PDR process and regular supervisory sessions	June 2020	Office Manager	
● Annual staff survey which forms the basis of a delivery plan	June 2020	Office Manager	● PDR process being considered to bring more independent assessment of these
● Training and development budget maintained		CFO	
● Skills matrix maintained	June 2020	Office Manager	● Need to refresh the matrix and better embed its use in the process of assigning new work
● Salary levels set at a reasonable market rate and in line with other OPCCs		CEO/CFO	
● Values and teamwork embedded and recruited to improving retention	Apr 2020	Head of Comms	● OPCC values reviewed and agreed waiting on development of supporting material/plan to launch at team meeting.

Risk	URN	Owner	Unmitigated Probability	Unmitigated Impact	Unmitigated Risk
Failure to deliver commissioned services	SR7	Head of C&P	4	4	16
			Mitigated Probability	Mitigated Impact	Mitigated Risk
			2	4	**8**
			Mitigated Risk change:		◀▶

Cause	Impact
● Vacancies and backlogs in in Lighthouse (the primary commissioned service) ● End of Home Office VAWG Transformation Fund risks continuity of provision after March 2020 ● Control Room Triage failing to deliver as expected ● Staff changes within the OPCC Commissioning & Partnerships Team	● Failure to support victims particularly vulnerable victims - PCP Priority 1 (SR2) ● Loss of public confidence in or awareness of OPCC (SR5) ● Relationship with Constabulary and partners ● Reduction or withdrawal of victims grant from Government ● Failure to devolve further funding/commissioning

MITIGATION

Controls	Review date	Owner	Commentary / Controls updates
● Maintain a sufficiently resourced and prioritised commissioning team within the OPCC.	June 2020	Head of C&P	● Senior Commissioning Officer will be on maternity leave from December 2019 however a new Support Officer started in Dec 19 and new Support Assistant in Jan 20. The temporary loss of the senior role is also being managed through the pipeline of work from the SLT into the team.
● Lighthouse victims' service jointly established with the Constabulary with regular review meetings.	June 2020	Head of C&P	● Recommendations for short-term improvements in Lighthouse were agreed at Sept PCB – this will continue to report back to PCB every month. Service needs to be at full capacity in order to properly evaluate it. Agreement to recruit to over establishment and use underspend to fund temporary additional posts in 20/21.
● Victim Services Provider forum and AWP Partnership Board are regular joint strategic meetings with commissioned services.		Head of C&P	
● Performance Framework includes commissioned services MoJ data to bring greater visibility and accountability of services.		Head of C&P	● Need to further improve the governance and decision making over commissioned services utilising the new performance framework.
● Co-commission, with the Constabulary, new approach to Out of Court Disposals and interventions.	June 2020	Senior C&P Officer	● ASCEND pilot went live Nov 2018. Two tier framework has been well adopted but overall numbers of OOCD have not seen a significant increase. Pathway and approach for hate crime still to be finalised and signed off. Evaluation to report in June 20.

Risk	URN	Owner	Unmitigated Probability	Unmitigated Impact	Unmitigated Risk
Failure to deliver effective and efficient collaborations with other forces	SR8	CEO	4	3	12
			Mitigated Probability	Mitigated Impact	Mitigated Risk
			4	3	**12**
			Mitigated Risk change:		◀▶

Cause	Impact
● 'Political' barriers to collaboration ● Reduced appetite for regional collaborations due to past failings ● Failure to agree effective models for collaboration ● Increased funding for police means the imperative to collaborate is not so pressing ● Ineffective governance and scrutiny over existing collaborations - lack of accountability ● Ineffective governance and ownership of regional projects and programmes ● Tension between local forces and collaborations in terms of competing interests and lack of uniformity of people and processes ● Lack of direct influence/control in order to make changes i.e. everything must be done by (multi-force) committee	● Governance failure as a duty of the PCC (SR1) ● Failure to deliver value for money ● Failure to deliver specific services provided by existing collaborations ● Inefficient compared to other regions/areas ● Criticism from HMICFRS ● Government scrutiny/intervention ● Lack of resilience otherwise provided by a collaboration ● Forced to accept others terms from future alliances or mergers

MITIGATION

Controls	Review date	Owner	Commentary / Controls updates
● Strategic Collaboration Governance ● Regional commissioning and programme boards and policy officer ● SWAP appointed as Internal Auditor (from April 2019) - working in partnership with other regional forces	June 2020	SPPO CFO CFO	● Given the reduced strategic oversight of the Collaboration Boards need to increase scrutiny within OPCC. Will be part of a revised performance framework under a new PCC. ● Remaining collaborations are largely mandated: - Regional Organised Crime Unit - Counter Terrorism Police - Forensics - Special Branch - NPAS - Tri Force Firearms Training - Major Crime Investigations

Risk	URN	Owner	Unmitigated Probability	Unmitigated Impact	Unmitigated Risk
Failure to deliver effective and efficient collaborations or outcomes with other partners	SR9	CEO	4	4	16
			Mitigated Probability	Mitigated Impact	Mitigated Risk
			3	3	**9**
			Mitigated Risk change:		◀▶

Cause	Impact
● Partner funding remains under pressure with financial settlements not keeping pace with inflation and demand. This increases the risk of demand and funding requests moving to the ASC and OPCC ● Failure to put in place effective governance and ownership of partnership working ● Differing priorities and leadership of agencies ● Lack of accountability ● Lack of meaningful 'live' information sharing	● Governance failure as a duty of the PCC (SR1) ● Failure to deliver the Police and Crime Plan (SR2) - particularly Priority 4 ● Failure to deliver a whole systems approach to crime and continue the 'revolving door' of offending and victimisation ● Failure to deliver value for money

MITIGATION

Controls	Review date	Owner	Commentary / Controls updates
● Representation on LCJB, CSPs, Children's Trusts, Health and Wellbeing Boards		CEO	
● Meetings (outside of Boards) with LA chairs/CEOs; CSP Chairs		CEO	
● Criminal Justice Transformation	March 2020	CSO (CJ)	● CJ Task Force is now live (taking over from Transformation Programme). This task force reports to the ASCJB which the PCC sits on/chairs.
● Resolve Programme (reducing re-offending) now operating at force and regional level	March 2020	Local / Regional SRO	● Local Resolve Programme extended to Sept 2020 – Regional SRO being recruited in Nov 2019
● Violence Reduction Units	Apr 2020	Senior C&P Officer	● HO funding granted for 2020/21 although details not known. Planning to maintain the current model with the same level of devolved funding. All areas have produced problem profiles and response strategies.
● Collaborate with Fire Authorities		CEO	
● Information sharing recognised by the VRU and reducing reoffending strategic groups as a key challenge - working with DSIC to try identify a solution	Apr 2020	Respective Strategic Groups	

Risk	URN	Owner	Unmitigated Probability	Unmitigated Impact	Unmitigated Risk
Failure to set an effective Police and Crime Plan	SR10	CEO	3	5	15
			Mitigated Probability	Mitigated Impact	Mitigated Risk
			2	4	**8**
			Mitigated Risk change:		◀▶

Cause	Impact
● PCC elections May 2020 - could result in a substantially revised or new plan - more likely given the certainty of a new PCC ● Failure to sufficiently assess needs ● Lack of data or poor data quality ● Ineffective working with the Constabulary	● Failure of governance particularly a key statutory requirement of the PCC (SR1) ● Lack of public confidence in or awareness of OPCC (SR5) ● Priorities, and therefore Constabulary service, fails to address local needs ● Inability to scrutinise the Constabulary effectively ● Ineffective working / loss of engagement with the Constabulary ● Ineffective working / loss of engagement with partners or other commissioned services

MITIGATION

Controls	Review date	Owner	Commentary / Controls updates
● Police and Crime Needs Assessment (PCNA) produced for 2019 which will be provided to all PCC candidates		CEO	● This is an emerging risk given the PCC elections. Failure to set a plan at all is the bigger impact but very unlikely: the bigger risk within this is ensuring the plan is effective.
● Revised PCNA will be produced ahead of any new plan being written		SPPO	
● OPCC will follow best practice outlined in 'APACE Police and Crime Plans - Guidance and Practice Advice' when setting a new plan. This best practice will also be briefed to new PCC.		SPPO	

Grant Thornton

9

Joint External Audit Plan

Year ending 31 March 2020

Police and Crime Commissioner for Avon and Somerset and Chief Constable for Avon and Somerset

19 March 2020

Contents

Your key Grant Thornton team members are:

Iain Murray

Director

T: 0207 728 3328

E: Iain.G.Murray@uk.gt.com

Gail Turner-Radcliffe

Audit Manager

T: 029 2034 7546

E: Gail.Turner-Radcliffe@uk.gt.com

Section **Page**

Appendix

The contents of this report relate only to the matters which have come to our attention, which we believe need to be reported to you as part of our audit planning process. It is not a comprehensive record of all the relevant matters, which may be subject to change, and in particular we cannot be held responsible to you for reporting all of the risks which may affect the PCC or Chief Constable or all weaknesses in your internal controls. This report has been prepared solely for your benefit and should not be quoted in whole or in part without our prior written consent. We do not accept any responsibility for any loss occasioned to any third party acting, or refraining from acting on the basis of the content of this report, as this report was not prepared for, nor intended for, any other purpose.

Grant Thornton UK LLP is a limited liability partnership registered in England and Wales: No.OC307742. Registered office: 30 Finsbury Square, London, EC2A 1AG. A list of members is available from our registered office. Grant Thornton UK LLP is authorised and regulated by the Financial Conduct Authority. Grant Thornton UK LLP is a member firm of Grant Thornton International Ltd (GTIL). GTIL and the member firms are not a worldwide partnership. Services are delivered by the member firms. GTIL and its member firms are not agents of, and do not obligate, one another and are not liable for one another's acts or omissions.

1. Introduction & headlines

Purpose

This document provides an overview of the planned scope and timing of the statutory audits of both the Police and Crime Commissioner for Avon and Somerset ('the PCC') and the Chief Constable for Avon and Somerset ('the Chief Constable') for those charged with governance. Those charged with governance are the PCC and the Chief Constable.

Respective responsibilities

The National Audit Office ('the NAO') has issued a document entitled Code of Audit Practice ('the Code'). This summarises where the responsibilities of auditors begin and end and what is expected from the audited body. Our respective responsibilities are also set out *in the Terms of Appointment and Statement of Responsibilities issued by Public Sector Audit Appointments (PSAA), the body responsible for appointing us as auditor of PCC and Chief Constable. We draw your attention to both of these documents on the PSAA website.*

Scope of our audit

The scope of our audits is set in accordance with the Code and International Standards on Auditing (ISAs) (UK). We are responsible for forming and expressing an opinion on the :

- PCC's, Chief Constable's and group's financial statements that have been prepared by management with the oversight of those charged with governance (the PCC and the Chief Constable); and
- Value for Money arrangements in place at each body for securing economy, efficiency and effectiveness in their use of resources.

The audit of the financial statements does not relieve management, the PCC or the Chief Constable of their responsibilities. It is the responsibility of the bodies to ensure that proper arrangements are in place for the conduct of its business, and that public money is safeguarded and properly accounted for. We have considered how the PCC and the Chief Constable are fulfilling these responsibilities.

Our audit approach is based on a thorough understanding of the PCC and the Chief Constable's business and is risk based.

Significant risks	Those risks requiring special audit consideration and procedures to address the likelihood of a material financial statement error have been identified as: • Management override of controls (presumed risk under ISA240) • Valuation of land and buildings • Valuation of net pension fund liability We will communicate significant findings on these areas as well as any other significant matters arising from the audit to you in our Audit Findings (ISA 260) Report.
Materiality	We have determined planning materiality to be £7.334m (PY £7.438m) for the group, the PCC and the Chief Constable, which equates to 2% of the Chief Constable's prior year gross expenditure for the year. We are obliged to report uncorrected omissions or misstatements other than those which are 'clearly trivial' to those charged with governance. Clearly trivial has been set at £0.367m (PY £0.372m).
Value for Money arrangements	Our risk assessment regarding your arrangements to secure value for money have identified the following VFM significant risks: • Financial planning and the medium term financial position.
Audit logistics	Our interim visit will take place in March 2020 and our final visit will take place in June and July 2020. Our key deliverables are this Audit Plan and our Audit Findings Report. Our proposed fee for the audit is £27,992 (PY: £27,992) for the PCC and £14,438 (PY: £14,438) for the Chief Constable, subject to management meeting our requirements set out on page 13. Fee variations of £8,500 (PY: £8,500) have been outlined on page 15.
Independence	We have complied with the Financial Reporting Council's Ethical Standard and we as a firm, and each covered person, confirm that we are independent and are able to express an objective opinion on the financial statements.

2. Key matters impacting our audit

DRAFT

Factors

Police officer uplift and funding uncertainty

In July 2019 the Government promised to recruit 20,000 extra police officers over the next three years. In September 2019 it announced a £750m increase in police funding as part of this commitment. Further details were set out in the 2020/21 Police Grant Report with £700m of this money being made available to PCCs in 2020/21 to fund the recruitment of 6,000 new officers, £168m of this money is ringfenced pending the achievement of local recruitment targets. Based on grant allocation Avon and Somerset's share would be 137 additional officers in 2021 and 368 additional officers by March 2023. This national expectation has been increased locally to 165 in 2021 and 403 by March 2023.

Police bodies will need to increase staff numbers and other costs to support the additional officers. The Government has made some funding available to support this growth. However there is some uncertainty about the extent of this funding in future periods.

The increase in funding associated with the uplift in police officer numbers presents a major opportunity for policing in the UK and gives ground for some cautious optimism.

There are challenges which the sector will need to manage as part of the uplift; such as increased political and public expectations, the need to adapt operating models based on shrinking officer numbers and the leadership and cultural challenges presented by a rapidly growing and relatively inexperienced workforce. There is also a risk that increased scrutiny and challenge on police officer numbers focuses long term decision making on the inputs to policing rather than outcomes.

Integrated PEEL Assessment

The most recent HMICFRS PEEL assessment was completed in 2018/19, Avon and Somerset Constabulary was graded as follows:

- Outstanding in relation to "The extent to which the force operates efficiently and sustainably is good"

- Good in relation to "The extent to which the force treats the public and its workforce legitimately is good"

- Good in relation to "The extent to which the force is effective at keeping people safe and reducing crime"

Financial reporting and audit – raising the bar

The Financial Reporting Council (FRC) has set out its expectation of improved financial reporting from organisations and the need for auditors to demonstrate increased scepticism and challenge, and to undertake more robust testing as detailed in Appendix 1.

Implementation of IFRS 16 - Leases

IFRS16 requires a leased asset, previously accounted for as an operating lease off balance sheet, to be recognised as a ‘right of use’ asset with a corresponding liability on the balance sheet from 1 April 2020. There is a requirement, under IAS8, to disclose the expected impact of this change in accounting treatment in the 2019/20 financial statements.

Our response

- We will consider your arrangements for managing and reporting your financial resources as part of our work in reaching our Value for Money conclusion.
- We will consider whether your financial position leads to material uncertainty about the going concern of the group, PCC and the Chief Constable and will review related disclosures in the financial statements.

As a firm, we are absolutely committed to meeting the expectations of the FRC with regard to audit quality and local government financial reporting. Our proposed work and fee, as set further in our Audit Plan and is subject to PSAA agreement.

We will assess the adequacy of your disclosure about the financial impact of implementing IFRS 16 – Leases from 1 April 2020.

3. Group audit scope and risk assessment

In accordance with ISA (UK) 600, as group auditor we are required to obtain sufficient appropriate audit evidence regarding the financial information of the components and the consolidation process to express an opinion on whether the group financial statements are prepared, in all material respects, in accordance with the applicable financial reporting framework.

Component	Individually Significant?	Audit Scope	Risks identified	Planned audit approach
Police and Crime Commissioner for Avon and Somerset	Yes	Audit of the financial information of the component using component materiality	See risks detailed on pages 6, 7 and 8	Full scope UK statutory audit performed by Grant Thornton UK LLP
Chief Constable for Avon and Somerset	Yes	Audit of the financial information of the component using component materiality	See risks detailed on pages 6, 7 and 8	Full scope UK statutory audit performed by Grant Thornton UK LLP

4. Significant risks identified

Significant risks are defined by ISAs (UK) as risks that, in the judgement of the auditor, require special audit consideration. In identifying risks, audit teams consider the nature of the risk, the potential magnitude of misstatement, and its likelihood. Significant risks are those risks that have a higher risk of material misstatement.

Risk	Risk relates to	Reason for risk identification	Key aspects of our proposed response to the risk
The revenue cycle includes fraudulent transactions (rebutted)	Group, PCC and the Chief Constable	Under ISA (UK) 240 there is a rebuttable presumed risk that revenue may be misstated due to the improper recognition of revenue. This presumption can be rebutted if the auditor concludes that there is no risk of material misstatement due to fraud relating to revenue recognition.	Having considered the risk factors set out in ISA240 and the nature of the revenue streams of the PCC and the Chief Constable, we have determined that the risk of fraud arising from revenue recognition can be rebutted, because: • there is little incentive to manipulate revenue recognition • opportunities to manipulate revenue recognition are very limited • the culture and ethical frameworks of public sector bodies, including the PCC, Chief Constable and group, mean that all forms of fraud are seen as unacceptable Therefore we do not consider this to be a significant risk for the PCC, Chief Constable or group.
Management over-ride of controls	Group, PCC and the Chief Constable	Under ISA (UK) 240 there is a non-rebuttable presumed risk that the risk of management over-ride of controls is present in all entities. We therefore identified management override of control, in particular journals, management estimates and transactions outside the course of business as a significant risk, which was one of the most significant assessed risks of material misstatement.	We will: • evaluate the design effectiveness of management controls over journals • analyse the journals listing and determine the criteria for selecting high risk unusual journals • test unusual journals recorded during the year and after the draft accounts stage for appropriateness and corroboration • gain an understanding of the accounting estimates and critical judgements applied made by management and consider their reasonableness with regard to corroborative evidence; and • evaluate the rationale for any changes in accounting policies, estimates or significant unusual transactions.

Significant risks identified

Risk	Risk relates to	Reason for risk identification	Key aspects of our proposed response to the risk
Valuation of land and buildings	Group and PCC	The PCC (and group) revalue land and buildings on an annual basis to ensure that the carrying value is not materially different from the current value or the fair value (for surplus assets) at the financial statements date via full valuations or on a desktop basis. This valuation represents a significant estimate by management in the financial statements due to the size of the numbers involved (£227 million) and the sensitivity of this estimate to changes in key assumptions. We therefore identified valuation of land and buildings as a significant risk, which was one of the most significant assessed risks of material misstatement.	We will: • evaluate management's processes and assumptions for the calculation of the estimate, the instructions issued to the valuation experts and the scope of their work; • evaluate the competence, capabilities and objectivity of the valuation expert; • discuss with the valuer the basis on which the valuations were carried out to ensure that the requirements of the Code are met; • challenge the information and assumptions used by the valuer to assess completeness and consistency with our understanding; • engage our own valuer to assess the instructions to the group's valuer, the group's valuer's report and the assumptions that underpin the valuation. • test, on a sample basis, revaluations made during the year to ensure they have been input correctly into the PCC (and group's) asset register • evaluate the assumptions made by management for any assets not revalued during the year and how management has satisfied themselves that these are not materially different to current value.

Significant risks identified

Risk	Risk relates to	Reason for risk identification	Key aspects of our proposed response to the risk
Valuation of the pension fund net liability	Group and Chief Constable	The group's pension fund net liability, as reflected in its balance sheet as the net defined benefit liability, represents a significant estimate in the financial statements. The pension fund net liability is considered a significant estimate due to the size of the numbers involved (£3.7 billion) in the group's balance sheet) and the sensitivity of the estimate to changes in key assumptions. We therefore identified valuation of the group's pension fund net liability as a significant risk, which was one of the most significant assessed risks of material misstatement.	We will: • update our understanding of the processes and controls put in place by management to ensure that the group's pension fund net liability is not materially misstated and evaluate the design of the associated controls; • evaluate the instructions issued by management to their management expert (an actuary) for this estimate and the scope of the actuary's work; • assess the competence, capabilities and objectivity of the actuary who carried out the group's pension fund valuation; • assess the accuracy and completeness of the information provided by the group to the actuary to estimate the liability; • test the consistency of the pension fund asset and liability and disclosures in the notes to the core financial statements with the actuarial report from the actuary; • undertake procedures to confirm the reasonableness of the actuarial assumptions made by reviewing the report of the consulting actuary (as auditor's expert) and performing any additional procedures suggested within the report; and • obtain assurances from the auditor of Somerset Pension Fund as to the controls surrounding the validity and accuracy of membership data; contributions data and benefits data sent to the actuary by the pension fund and the fund assets valuation in the pension fund financial statements.

.

5. Other risks identified

Risk	Risk relates to	Reason for risk identification	Key aspects of our proposed response to the risk
International Financial Reporting Standard (IFRS) 16 Leases – (issued but not adopted)	Group	The public sector will implement this standard from 1 April 2020. It will replace IAS 17 Leases, and the three interpretations that supported its application (IFRIC 4, Determining whether an Arrangement contains a Lease, SIC-15, Operating Leases – Incentives, and SIC-27 Evaluating the Substance of Transactions Involving the Legal Form of a Lease). Under the new standard the current distinction between operating and finance leases is removed for lessees and, subject to certain exceptions, lessees will recognise all leases on their balance sheet as a right of use asset and a liability to make the lease payments. In accordance with IAS 8 and paragraph 3.3.4.3 of the Code disclosures of the expected impact of IFRS 16 should be included in the entity's 2019/20 financial statements. The Code adapts IFRS 16 and requires that the subsequent measurement of the right of use asset where the underlying asset is an item of property, plant and equipment is measured in accordance with section 4.1 of the Code.	We will: • Evaluate the processes the entity has adopted to assess the impact of IFRS16 on its 2020/21 financial statements and whether the estimated impact on assets, liabilities and reserves has been disclosed in the 2019/20 financial statements. • Assess the completeness of the disclosures made by the Authority in its 2019/20 financial statements with reference to The Code and CIPFA/LASAAC Local Authority Leasing Briefings.

We will communicate significant findings on these areas as well as any other significant matters arising from the audit to you in our Audit Findings Report in July 2020.

6. Other matters

Other work

In audit responsibilities, as follows:

- We read your Narrative Reports and Annual Governance Statements to check that they are consistent with the financial statements on which we give an opinion and our knowledge of the PCC and Chief Constable.
- We carry out work to satisfy ourselves that disclosures made in your Annual Governance Statements are in line with guidance issued by CIPFA.
- We carry out work on your consolidation schedules for the Whole of Government Accounts process in accordance with NAO group audit instructions.
- We consider our other duties under legislation and the Code, as and when required, including:
    - Giving electors the opportunity to raise questions about your 2019/20 financial statements, consider and decide upon any objections received in relation to the 2019/20 financial statements;
    - Issue of a report in the public interest or written recommendations to the PCC or the Chief Constable under section 24 of the Act, copied to the Secretary of State.
    - Application to the court for a declaration that an item of account is contrary to law under Section 28 or for a judicial review under Section 31 of the Act; or
    - Issuing an advisory notice under Section 29 of the Act.
- We certify completion of our audit.

Other material balances and transactions

Under International Standards on Auditing, "irrespective of the assessed risks of material misstatement, the auditor shall design and perform substantive procedures for each material class of transactions, account balance and disclosure". All other material balances and transaction streams will therefore be audited. However, the procedures will not be as extensive as the procedures adopted for the risks identified in this report.

Going concern

As auditors, we are required to “obtain sufficient appropriate audit evidence about the appropriateness of management's use of the going concern assumption in the preparation and presentation of the financial statements and to conclude whether there is a material uncertainty about the entity's ability to continue as a going concern” (ISA (UK) 570). We will review management's assessment of the going concern assumption and material uncertainties, and evaluate the disclosures in the financial statements.

7. Materiality

The concept of materiality

The concept of materiality is fundamental to the preparation of the financial statements and the audit process and applies not only to the monetary misstatements but also to disclosure requirements and adherence to acceptable accounting practice and applicable law. Misstatements, including omissions, are considered to be material if they, individually or in the aggregate, could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements.

Materiality for planning purposes

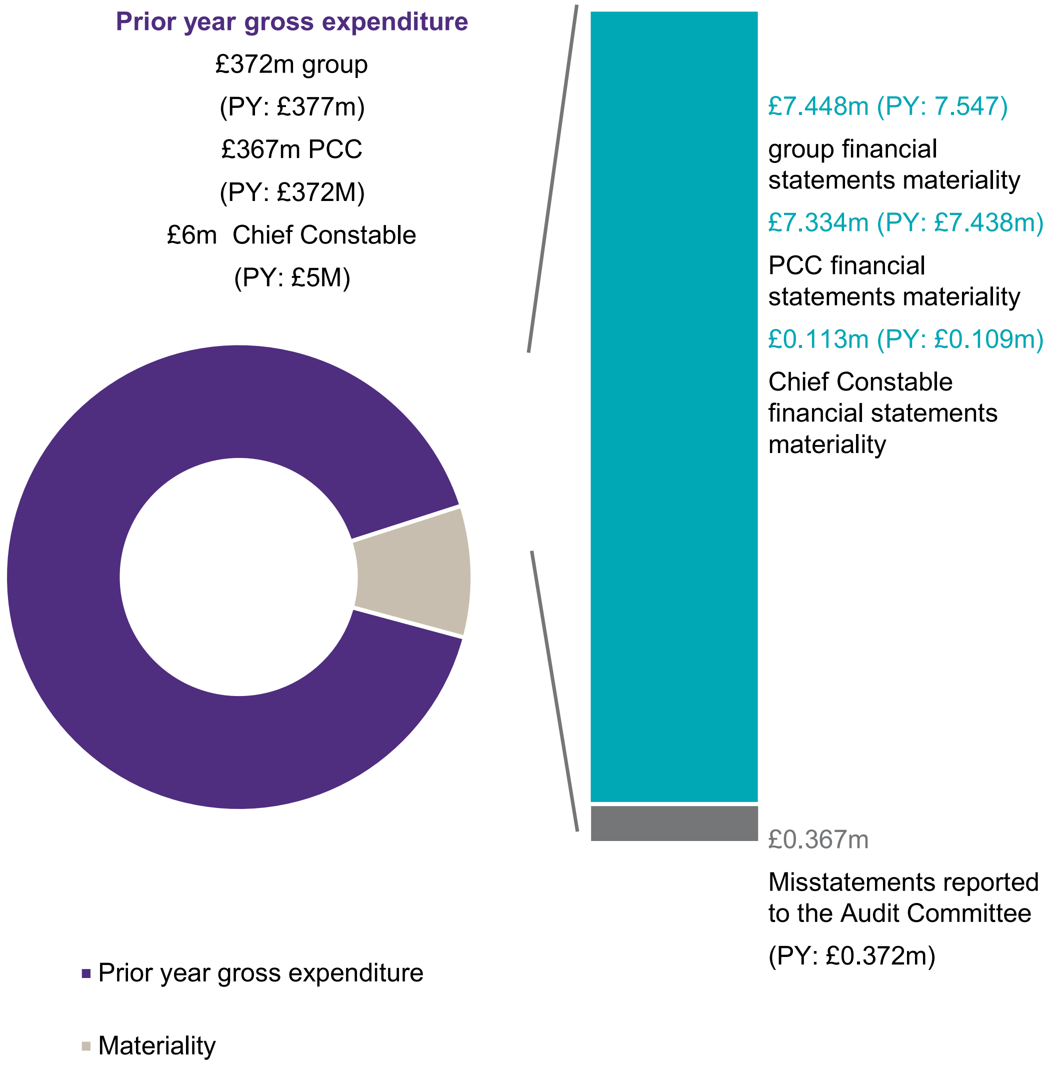
We have determined financial statement materiality's based on a proportion of the gross expenditure of the group, the PCC and the Chief Constable for the financial year. In the prior year we used the same benchmark. For our audit testing purposes we apply the lowest of these materiality's, which is £7.334m (PY £7.438m), which equates to 2% of the Chief Constable's prior year gross expenditure or the year. We design our procedures to detect errors in specific accounts at a lower level of precision which we have determined to be £25k for Senior officer remuneration.

We reconsider planning materiality if, during the course of our audit engagement, we become aware of facts and circumstances that would have caused us to make a different determination of planning materiality.

Matters we will report to the PCC and Chief Constable

Whilst our audit procedures are designed to identify misstatements which are material to our opinion on the financial statements as a whole, we nevertheless report to the PCC and Chief Constable any unadjusted misstatements of lesser amounts to the extent that these are identified by our audit work. Under ISA 260 (UK) 'Communication with those charged with governance', we are obliged to report uncorrected omissions or misstatements other than those which are 'clearly trivial' to those charged with governance. ISA 260 (UK) defines 'clearly trivial' as matters that are clearly inconsequential, whether taken individually or in aggregate and whether judged by any quantitative or qualitative criteria. In the context of the group, the PCC and the Chief Constable, we propose that an individual difference could normally be considered to be clearly trivial if it is less than £0.367m (PY £0.372m).

If management have corrected material misstatements identified during the course of the audit, we will consider whether those corrections should be communicated to the PCC and Chief Constable to assist it in fulfilling its governance responsibilities.



Prior year gross expenditure

£372m group

(PY: £377m)

£367m PCC

(PY: £372M)

£6m Chief Constable

(PY: £5M)

£7.448m (PY: 7.547)

group financial statements materiality

£7.334m (PY: £7.438m)

PCC financial statements materiality

£0.113m (PY: £0.109m)

Chief Constable financial statements materiality

£0.367m

Misstatements reported to the Audit Committee

(PY: £0.372m)

■ Prior year gross expenditure

■ Materiality

8. Value for Money arrangements

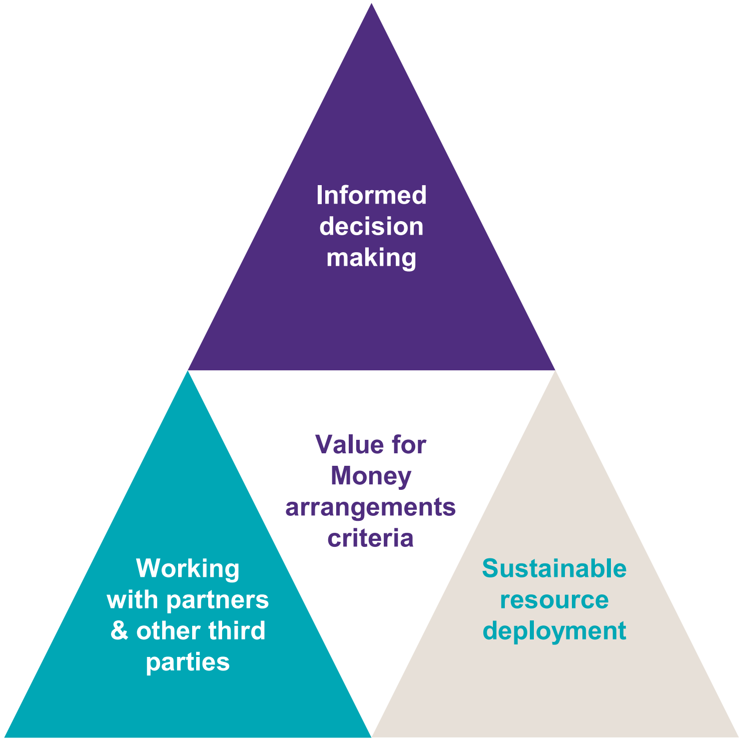
Background to our VFM approach

The NAO issued its guidance for auditors on Value for Money work in November 2017. The guidance states that for Police bodies, auditors are required to give a conclusion on whether the PCC and the Chief Constable each have proper arrangements in place to secure value for money.

The guidance identifies one single criterion for auditors to evaluate:

“In all significant respects, the audited body takes properly informed decisions and deploys resources to achieve planned and sustainable outcomes for taxpayers and local people.”

This is supported by three sub-criteria, as set out below:



Informed decision making
Value for Money arrangements criteria
Working with partners & other third parties
Sustainable resource deployment

Significant VFM risks

Those risks requiring audit consideration and procedures to address the likelihood that proper arrangements are not in place at the PCC or the Chief Constable to deliver value for money.

⚠

Medium Term Financial Planning

The latest police finance settlement announced in January 2020 provides PCC’s with increased funding via police grant and the option to raise additional monies through an increase in the policing precept.

Whilst this settlement was largely better than expected by the sector, financial challenges still remain in the medium term due to increasing and more complex demand and other cost pressures such as increases to police pension contributions.

The increased funding also comes with the expectation that the constabulary will increase police officer numbers in the year ahead.

The PCC and Chief Constable need to continue to plan prudently for the future to ensure that they can continue to set balanced budgets in line with their statutory responsibilities.

We will:

review the outturn revenue position and consider the impact on our responsibilities, including the balance between recurrent and non-recurrent steps taken in delivering outturn;

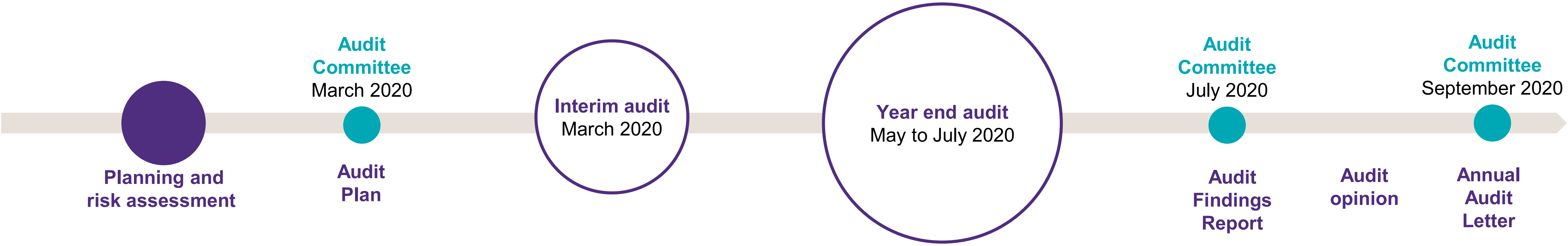
consider the arrangements for monitoring and managing the delivery of budget and savings plans for 2019/20; and

review the arrangements for developing and agreeing the 2020/21 budgets and updated Medium Term Financial Plan.

review the Constabulary’s plans for recruitment to ensure that these are aligned to the future financial plans.

review the capital and borrowing plans to ensure these are sustainable into the future

9. Audit logistics & team


Planning and risk assessment
Audit Committee March 2020
Audit Plan
Interim audit March 2020
Year end audit May to July 2020
Audit Committee July 2020
Audit Findings Report
Audit opinion
Audit Committee September 2020
Annual Audit Letter

Iain Murray, Engagement Lead

Iain leads our relationship with you and is a key contact for the PCC, Chief Constable, Chief Finance Officers and the Joint Audit Committee. Iain takes overall responsibility for the delivery of a high quality audit, meeting the highest professional standards and adding value.

Gail Turner-Radcliffe, Audit Manager

Gail's role involves overseeing the day to day planning and execution of the audit, ensuring the audit requirements are fully complied with and producing reports for the Joint Audit Committee. She will respond to ad-hoc queries whenever raised and meet regularly with the Chief Finance Officers and members of the finance team.

Client responsibilities

Where clients do not deliver to the timetable agreed, we need to ensure that this does not impact on audit quality or absorb a disproportionate amount of time, thereby disadvantaging other clients. Where the elapsed time to complete an audit exceeds that agreed due to a client not meeting its obligations we will not be able to maintain a team on site. Similarly, where additional resources are needed to complete the audit due to a client not meeting their obligations we are not able to guarantee the delivery of the audit to the agreed timescales. In addition, delayed audits will incur additional audit fees.

Our requirements

To minimise the risk of a delayed audit, you need to ensure that you:

- produce draft financial statements of good quality by the deadline you have agreed with us, including all notes, the narrative report and the Annual Governance Statement
- ensure that good quality working papers are available at the start of the audit, in accordance with the working paper requirements schedule that we have shared with you
- ensure that the agreed data reports are available to us at the start of the audit and are reconciled to the values in the accounts, in order to facilitate our selection of samples
- ensure that all appropriate staff are available on site throughout (or as otherwise agreed) the planned period of the audit
- respond promptly and adequately to audit queries.

10. Audit fees

.

Planned audit fees 2019/20

Across all sectors and firms, the FRC has set out its expectation of improved financial reporting from organisations and the need for auditors to demonstrate increased scepticism and challenge and to undertake additional and more robust testing. Within the public sector, where the FRC has recently assumed responsibility for the inspection of local government audit, the regulator requires that all audits achieve a 2A (few improvements needed) rating.

Our work across the sector in 2018/19 has highlighted areas where local government financial reporting, in particular, property, plant and equipment and pensions, needs to be improved. We have also identified an increase in the complexity of local government financial transactions. Combined with the FRC requirement that 100% of audits achieve a 2A rating this means that additional audit work is required. We have set out below the expected impact on our audit fee. The table overleaf provides more details about the areas where we will be undertaking further testing.

As a firm, we are absolutely committed to meeting the expectations of the FRC with regard to audit quality and local government financial reporting. Our proposed work and fee at the planning stage, as set out below and with further analysis overleaf, has been shared with the Chief Finance Officer and is subject to PSAA agreement.

	Actual Fee 2017/18	Actual Fee 2018/19	Proposed fee 2019/20
PCC Audit	£36,353	£27,992	£27,992
Chief Constable Audit	£18,750	£14,438	£14,438
Fee Variations	-	£8,500	£8,500
Total audit fees (excluding VAT)	**£55,103**	**£50,930**	**£50,930**

Assumptions:
In setting the above fees, we have assumed that management will:

- prepare a good quality set of accounts, supported by comprehensive and well presented working papers which are ready at the start of the audit
- provide appropriate analysis, support and evidence to support all critical judgements and significant judgements made during the course of preparing the financial statements
- provide early notice of proposed complex or unusual transactions which could have a material impact on the financial statements.

Relevant professional standards:
In preparing our fee estimate, we have had regard to all relevant professional standards, including paragraphs 4.1 and 4.2 of the FRC's Ethical Standard which stipulate that the Engagement Lead (Key Audit Partner) must set a fee sufficient to enable the resourcing of the audit with staff of appropriate skills, time and abilities to deliver an audit to the required professional standard.

Audit fee variations – Further analysis

Planned audit fees

The table below shows the planned variations to the original scale fee for 2019/20 based on our best estimate at the audit planning stage. Further issues identified during the course of the audit may incur additional fees.

Audit area	£	Rationale for fee variation
Scale fee	42,430	
Pensions – valuation of net pension liabilities under International Auditing Standard (IAS) 19	1,750	The Financial Reporting Council (FRC) has highlighted that the quality of work by all audit firms in respect of IAS 19 needs to improve across public sector audits. Accordingly, we plan to increase the level of scope and coverage of our work in respect of IAS 19 this year to reflect the expectations of the FRC and ensure we issue a safe audit opinion. Specifically, we have increased the granularity, depth and scope of coverage, with increased levels of sampling, additional levels of challenge and explanation sought, and heightened levels of documentation and reporting.
PPE Valuation – work of experts	2,500	As above, the FRC has also determined that auditors need to improve the quality of audit challenge on PPE valuations across the sector. We have therefore engaged our own audit expert. We estimate that the cost of the auditors expert will be in the region of £5000.
PPE	1,750	As above, increased the volume and scope of our audit work to ensure an adequate level of audit scrutiny and challenge over the assumptions that underpin PPE valuations.
Increased challenge and depth of work	2,500	The FRC has now set a 100% target for all audits (including local audits) to achieve a '2a' quality grading. Its threshold for achieving a '2a' is challenging and failure to achieve this level is reputationally damaging for individual engagement leads and their firm. Non-achievement of the standard can result in enforcement action, including fines and disqualification, by the FRC. Inevitably, we need to increase the managerial oversight to manage this risk. In addition, you should expect the audit team to exercise even greater challenge of management in areas that are complex, significant or highly judgmental.

11. Independence & non-audit services

Auditor independence

Ethical Standards and ISA (UK) 260 require us to give you timely disclosure of all significant facts and matters that may bear upon the integrity, objectivity and independence of the firm or covered persons relating to our independence. We encourage you to contact us to discuss these or any other independence issues with us. We will also discuss with you if we make additional significant judgements surrounding independence matters.

We confirm that there are no significant facts or matters that impact on our independence as auditors that we are required or wish to draw to your attention. We have complied with the Financial Reporting Council's Ethical Standard and we as a firm, and each covered person, confirm that we are independent and are able to express an objective opinion on the financial statements.

We confirm that we have implemented policies and procedures to meet the requirements of the Financial Reporting Council's Ethical Standard and we as a firm, and each covered person, confirm that we are independent and are able to express an objective opinion on the financial statements. Further, we have complied with the requirements of the National Audit Office's Auditor Guidance Note 01 issued in December 2017 and PSAA's Terms of Appointment which set out supplementary guidance on ethical requirements for auditors of local public bodies.

Other services provided by Grant Thornton

For the purposes of our audit we have made enquiries of all Grant Thornton UK LLP teams providing services to the PCC and the Chief Constable. No other services were identified.

Appendix A: Audit Quality – national context

What has the FRC said about Audit Quality?

The Financial Reporting Council (FRC) publishes an annual Quality Inspection of our firm, alongside our competitors. The Annual Quality Review (AQR) monitors the quality of UK Public Interest Entity audits to promote continuous improvement in audit quality.

All of the major audit firms are subject to an annual review process in which the FRC inspects a small sample of audits performed from each of the firms to see if they fully conform to required standards.

The most recent report, published in July 2019, shows that the results of commercial audits taken across all the firms have worsened this year. The FRC has identified the need for auditors to:

- improve the extent and rigour of challenge of management in areas of judgement
- improve the consistency of audit teams' application of professional scepticism
- strengthen the effectiveness of the audit of revenue
- improve the audit of going concern
- improve the audit of the completeness and evaluation of prior year adjustments.

The FRC has also set all firms the target of achieving a grading of '2a' (limited improvements required) or better on all FTSE 350 audits. We have set ourselves the same target for public sector audits from 2019/20.

Other sector wide reviews

Alongside the FRC, other key stakeholders including the Department for Business, energy and Industrial Strategy (BEIS) have expressed concern about the quality of audit work and the need for improvement. A number of key reviews into the profession have been undertaken or are in progress. These include the review by Sir John Kingman of the Financial Reporting Council (Dec 2018), the review by the Competition and Markets authority of competition within the audit market, the ongoing review by Sir Donald Brydon of external audit, and specifically for public services, the Review by Sir Tony Redmond of local authority financial reporting and external audit. As a firm, we are contributing to all these reviews and keen to be at the forefront of developments and improvements in public audit.

What are we doing to address FRC findings?

In response to the FRC's findings, the firm is responding vigorously and with purpose. As part of our Audit Investment Programme (AIP), we are establishing a new Quality Board, commissioning an independent review of our audit function, and strengthening our senior leadership at the highest levels of the firm, for example through the appointment of Fiona Baldwin as Head of Audit. We are confident these investments will make a real difference.

We have also undertaken a root cause analysis and put in place processes to address the issues raised by the FRC. We have already implemented new training material that will reinforce the need for our engagement teams to challenge management and demonstrate how they have applied professional scepticism as part of the audit. Further guidance on auditing areas such as revenue has also been disseminated to all audit teams and we will continue to evolve our training and review processes on an ongoing basis.

What will be different in this audit?

We will continue working collaboratively with you to deliver the audit to the agreed timetable whilst improving our audit quality. In achieving this you may see, for example, an increased expectation for management to develop properly articulated papers for any new accounting standard, or unusual or complex transactions. In addition, you should expect engagement teams to exercise even greater challenge management in areas that are complex, significant or highly judgmental which may be the case for accounting estimates, going concern, related parties and similar areas. As a result you may find the audit process even more challenging than previous audits. These changes will give the audit committee – which has overall responsibility for governance - and senior management greater confidence that we have delivered a high quality audit and that the financial statements are not materially misstated. Even greater challenge of management will also enable us to provide greater insights into the quality of your finance function and internal control environment and provide those charged with governance confidence that a material misstatement due to fraud will have been detected.

We will still plan for a smooth audit and ensure this is completed to the timetable agreed. However, there may be instances where we may require additional time for both the audit work to be completed to the standard required and to ensure management have appropriate time to consider any matters raised. This may require us to agree with you a delay in signing the announcement and financial statements. To minimise this risk, we will keep you informed of progress and risks to the timetable as the audit progresses.

We are absolutely committed to delivering audit of the highest quality and we should be happy to provide further detail about our improvement plans should you require it.

Grant Thornton

grantthornton.co.uk