GREATER MANCHESTER JOINT AUDIT PANEL
(POLICE AND CRIME)

PART A

1. Terms of Reference - Proposed Changes [p] [3 - 13] Internal Audit
2. Corporate Risk Management Arrangements in GMP – Updated Position [p] [15 - 17] GMP
3. HMICFRS iOPS Report [p] [19 - 42] GMP
4. GMP Anti-Fraud Policy – Updated Position [p] [43 ] GMP
5. Progress against the Internal Audit Plan 2018/20 [p] [45-57] Internal Audit
   Report of the Head of Audit and Assurance
6. Internal Audit Plan 2020/21 [p] [59 - 62] Internal Audit
   Report of the Head of Audit and Assurance
7. GMPs 2019/20 Audit Strategy Memorandum [p] [63 -79] Mazars

EXCLUSION OF PRESS AND PUBLIC

That, under section 100 (A)(4) of the Local Government Act 1972 the press and public should be excluded from the meeting for the following items on business on the grounds that this involves the likely disclosure of exempt information, as set out in paragraph 3, Part 1, Schedule 12A of the Local Government Act 1972 and that the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

PART B

8. Internal Audit Action Tracker Report
   Report of the Head of Audit and Assurance Internal Audit
9. GMPs Risk Register GMP
   i. Current Risk Register
   ii. New Risk Register
   iii. Force Template
10. Draft Anti-Fraud, Corruption and Bribery Policy GMP
11. The Force’s Response to the HMICFRS iOPS Recommendations
   Deputy Mayor Briefing GMP

[p] Paper attached
This page is intentionally left blank
Overview:
The purpose of this report is to obtain approval of proposed changes to the Terms of Reference for the Joint Audit Panel.

Detail:
The Joint Audit Panel is a key cornerstone of the corporate governance process. The Panel provides an independent and high-level focus on the audit, assurance and reporting arrangements that underpin good governance and financial standards.

The Terms of Reference summarises the core functions of the Joint Audit Panel and the protocols in place to enable it to operate independently, robustly and effectively.

In line with the approved Terms of Reference that have been in place since December 2018 there is a requirement that this document should be reviewed on an annual basis.

The proposed changes are in line with the CIPFA’s (The Chartered Institute of Public Finance and Accounting) latest model terms of reference for Police.

It ensures that the terms of reference are in accordance with the revised Financial Management Code of Practice for the Police Forces of England and Wales (Home Office, 2018 and that the Panel remain an advisory body.

The revised Terms of Reference is attached at Appendix A.

The existing Terms of Reference is attached at Appendix B.

Risk:

<table>
<thead>
<tr>
<th>Risk</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-compliance with the CIPFA’s guidance on the function and operation of the Joint Audit Panel.</td>
<td>Adoption of the latest model of terms of reference suggested by CIPFA.</td>
</tr>
</tbody>
</table>
Recommendations:

Members are asked to approve the revisions to the Audit Panel Terms of Reference, as detailed in this report.

Attachments:

Appendix A - Revised Terms of Reference
Appendix B - Existing Terms of Reference marked up with proposed changes
Revised Terms of Reference for the Greater Manchester Joint Audit Panel (Police and Crime)

PURPOSE

The Joint Audit Panel is a key component of the Deputy Mayor for Policing and Crime (the Deputy Mayor) and the Chief Constable’s for Greater Manchester corporate governance framework. It provides an independent and high-level focus on the audit, assurance and reporting arrangements that underpin good governance and financial standards.

The purpose of the Panel is to provide independent assurance on the adequacy of the risk management framework, the internal control environment and the integrity of the financial reporting and annual governance processes in operation within the Chief Constable’s Corporation Sole and the GM Mayor’s PCC functions.

Governance, Risk and Control

The panel will Review the corporate governance arrangements against the Delivering Good Governance in Local Government: Framework (CIPFA/Solace, 2016) (‘the Framework’) including the ethical framework and consider the local code of governance.

1. Review the Annual Governance Statement prior to approval and consider whether it properly reflects the governance, risk and control environment and supporting assurances and identify any actions required for improvement.

2. Consider the arrangements to secure value for money and review assurances and assessments on the effectiveness of these arrangements.

3. Consider the framework of assurance and ensure that it adequately addresses the risks and priorities of the Police, Crime and Criminal Justice Directorate and the constabulary.

4. Monitor the effective development and operation of risk management processes, review the risk profile of the Force and PCC functions, and monitor progress of the Deputy Mayor / the Chief Constable in addressing risk-related issues reported to them.

5. Consider reports on the effectiveness of internal controls and monitor the implementation of agreed actions.

6. Review arrangements for the assessment of fraud risks and potential harm from fraud and corruption and monitor the effectiveness of the counter fraud strategy, actions and resources.

7. Review the governance and assurance arrangements for significant partnerships or collaborations.
Internal Audit

The Panel will:

8. Annually review the internal audit charter and resources.
9. Consider the adequacy of the performance of the internal audit service and its independence.
10. Monitor (but not direct) the Internal Audit Plan, relating to the Force and advise on items for inclusion in the plan.
11. Receive progress reports on the Internal Audit work plan and advising the Deputy Mayor and Chief Constable when appropriate action is not taken in response to audit findings, particularly in areas of high risk;
12. Consider the Head of Internal Audit’s annual report and opinion, and a regular summary of the progress of internal audit activity against the audit plan, and the level of assurance it can give over corporate governance arrangements.
13. Consider the Head of Internal Audit’s statement of the level of conformance with the Public Sector Internal Audit Standards and the results of the Quality Assurance Improvement Programme that support the statement – these will indicate the reliability of the conclusions of internal audit.
14. Consider internal audit reports and such detailed reports as the panel may request from the Deputy Mayor / Chief Constable, including issues raised or recommendations made by the internal audit service, management response and progress with agreed actions.
15. Consider a report on the effectiveness of internal audit to support the Annual Governance Statement where required to do so by the Accounts and Audit Regulations 2015.
16. Consider any impairments to independence or objectivity arising from additional roles or responsibilities outside of internal auditing of the Head of Internal Audit. To make recommendations on safeguards to limit such impairments and periodically review their operation.

External Audit

The panel will:

17. Support the independence of external audit through consideration of the External Auditor’s annual assessment of its independence and review of any issues raised by either PSAA or the auditor panel as appropriate.
18. Comment on the scope and depth of External Audit work, its independence and whether it gives satisfactory value for money.
19. Consider the external auditor’s annual management letter, relevant reports and the report to those charged with governance.
20. Consider specific reports as agreed with the External Auditor.
21. Advise and recommend on the effectiveness of relationships between external and internal audit and other inspection agencies or relevant bodies.
**Financial Reporting**

The Panel will:

22. Review the annual statement of accounts. Specifically, to consider whether appropriate accounting policies have been followed and whether there are concerns arising from the financial statements or from the audit of the financial statements that need to be brought to the attention of the Deputy Mayor / Chief Constable.

23. Consider the External Auditor’s report to those charged with governance on issues arising from the audit of the financial statements.

**Accountability Arrangements**

In line with the GMCA Constitution, the Panel will:

24. On a timely basis report to the Deputy Mayor and the Chief Constable with its advice and recommendations in relation to any matters that it considers relevant to governance, risk management and financial management.

25. Report to the Deputy Mayor and the Chief Constable on its findings, conclusions and recommendations concerning the adequacy and effectiveness of their governance, risk management and internal control frameworks, financial reporting arrangements, and internal and external audit functions.

26. Review its performance against its terms of reference and objectives on an annual basis and report the results of this review to the PCC and the Chief Constable.

27. Report to the GMCA Audit Committee on Police Fund activity and assurance.

28. Publish an annual report on the work of the panel.

**Membership**

The Panel will comprise a maximum of five members including the Chair, who are independent of the Chief Constable and the Mayor. The meeting will only be quorate if at least three members are in attendance.

Initial term of office to be three years with up to a further three years on renewal.

Chair to be agreed by the Deputy Mayor and Chief Constable after considering applications for those interested.

**Meetings**

The Audit Panel will meet at least four times a year.

The Chair of the Panel may convene additional meetings, as they deem necessary.

Audit Panel meetings will normally be attended by, the Chief Finance Officer(s), or appropriate senior and qualified substitute, the Chief Constable or appropriate senior and qualified substitute, the Head of Internal Audit and the appointed External Auditor.
The Panel will have the right to call, as required, any other GMP police officers/staff and officers with responsibility for the GM Mayors Police, Crime and Criminal Justice functions, including the Mayor/Deputy Mayor.

**Skills**

To aid the Panel in delivering its purpose all Members will be required to undergo appropriate training which will be funded by the authority.

**Review**

The Panel will review its terms of reference annually.
GREATER MANCHESTER JOINT AUDIT PANEL  
(POLICE AND CRIME)  

TERMS OF REFERENCE  

PURPOSE  
The Joint Audit Panel is a key component of the Deputy Mayor for Policing and Crime (the Deputy Mayor) and the Chief Constable’s for Greater Manchester corporate governance framework. It provides an independent and high-level focus on the audit, assurance and reporting arrangements that underpin good governance and financial standards.

To provide independent assurance on the adequacy of the risk management framework, the internal control environment and the integrity of the financial reporting and annual governance processes in operation within the Chief Constable’s Corporation Sole and the functions of the GMCA responsible for administering the Police Fund (income, expenditure, assets, liabilities).

CORE FUNCTIONS  
REFRESH NOTE: The Core Function Section has been replaced by the specific activities that enable the Panel to deliver its Core Functions these are shown under the following headings, Governance, Risk and Control, Internal Audit, External Audit, Financial Reporting, Accountability Arrangements i.e. ‘How’ the Core functions are delivered. A cross check has been undertaken between this and the new version and all the core functions listed here are covered in the new ToR.

- To ensure that assurance statements, including the Annual Governance Statement, properly reflect the risk environment and any actions required to improve it, and demonstrate how governance supports the achievements of the Chief Constable’s objectives;
- To oversee the independence, objectivity, performance and professionalism of the internal audit function;
- To support the effectiveness of the internal audit process;
- To promote the effective use of internal audit within the assurance framework;
- To consider the effectiveness of the authority’s risk management arrangements and the control environment;
- To review the risk profile of the organisation and assurances that action is being taken on risk-related issues, including partnerships with other organisations;
- To monitor the effectiveness of the control environment, including arrangements for ensuring value for money and for managing the authority’s exposure to the risks of fraud and corruption;
- To receive the reports and recommendations of external audit and inspection agencies and consider their implications for governance, risk management or control;
- To support effective relationships between external audit and internal audit, inspection agencies and other relevant bodies, and encourage the active promotion of the value of the audit process;
To review the financial statements, external auditor’s opinion and report to the authority, and monitor management action in response to the issues raised by external audit.

**Governance, Risk and Control**

The panel will provide advice and recommendations to the Deputy Mayor / the Chief Constable in relation to the following areas:

29. Review the corporate governance arrangements against the Delivering Good Governance in Local Government: Framework (CIPFA/Solace, 2016) (‘the Framework’) including the ethical framework and consider the local code of governance.

30. Review the Annual Governance Statement prior to approval and consider whether it properly reflects the governance, risk and control environment and supporting assurances and identify any actions required for improvement.

31. Consider the arrangements to secure value for money and review assurances and assessments on the effectiveness of these arrangements.

32. Consider the framework of assurance and ensure that it adequately addresses the risks and priorities of the Police, Crime and Criminal Justice Directorate and the constabulary.

33. Monitor the effective development and operation of risk management, review the risk profile, and monitor progress of the Deputy Mayor / the Chief Constable in addressing risk-related issues reported to them.

34. Consider reports on the effectiveness of internal controls and monitor the implementation of agreed actions.

35. Review arrangements for the assessment of fraud risks and potential harm from fraud and corruption and monitor the effectiveness of the counter fraud strategy, actions and resources.

36. To review the governance and assurance arrangements for significant partnerships or collaborations.

**Internal Audit**

The Panel will:

37. Annually review the internal audit charter and resources.

38. Oversee the appointment and consider the adequacy of the performance of the internal audit service and its independence.

39. Monitor (but not direct) the Internal Audit Plan, relating to the Force and, where deemed appropriate by the Treasurer to the GMCA, the Mayor’s PCC functions, and advise on items for inclusion in the plan.

40. Receive progress reports on the Internal Audit work plan and advising the Deputy Mayor and Chief Constable when appropriate action is not taken in response to audit findings, particularly in areas of high risk;

41. Consider the Head of Internal Audit’s annual report and opinion, and a regular summary of the progress of internal audit activity against the audit plan, and the level of assurance it can give over corporate governance arrangements.
42. To consider the Head of Internal Audit’s statement of the level of conformance with the Public Sector Internal Audit Standards and the results of the Quality Assurance Improvement Programme that support the statement – these will indicate the reliability of the conclusions of internal audit.

43. Consider summaries of internal audit reports and such detailed reports as the panel may request from the Deputy Mayor / Chief Constable, including issues raised or recommendations made by the internal audit service, management response and progress with agreed actions.

44. Consider a report on the effectiveness of internal audit to support the Annual Governance Statement where required to do so by the Accounts and Audit Regulations 2015.

45. To consider any impairments to independence or objectivity arising from additional roles or responsibilities outside of internal auditing of the Head of Internal Audit. To make recommendations on safeguards to limit such impairments and periodically review their operation

External Audit

The panel will:

46. Support the independence of external audit through consideration of the External Auditor’s annual assessment of its independence and review of any issues raised by either PSAA or the auditor panel as appropriate.

47. Comment on the scope and depth of External Audit work, its independence and whether it gives satisfactory value for money.

48. Consider the external auditor’s annual management letter, relevant reports and the report to those charged with governance.

49. Consider specific reports as agreed with the External Auditor.

50. Advise and recommend on the effectiveness of relationships between external and internal audit and other inspection agencies or relevant bodies.

Financial Reporting

The Panel will:

51. Review the annual statement of accounts. Specifically, to consider whether appropriate accounting policies have been followed and whether there are concerns arising from the financial statements or from the audit of the financial statements that need to be brought to the attention of the Deputy Mayor / Chief Constable.

52. Consider the External Auditor’s report to those charged with governance on issues arising from the audit of the financial statements.

Accountability Arrangements

In line with the GMCA Constitution, the Panel will do the following:

53. On a timely basis report to the Deputy Mayor and the Chief Constable with its advice and recommendations in relation to any matters that it considers relevant to governance, risk management and financial management.
54. Report to the Deputy Mayor and the Chief Constable on its findings, conclusions and recommendations concerning the adequacy and effectiveness of their governance, risk management and internal control frameworks, financial reporting arrangements, and internal and external audit functions.

55. Review its performance against its terms of reference and objectives on an annual basis and report the results of this review to the PCC and the Chief Constable.

56. Publish an annual report on the work of the panel.

**REQUIREMENTS**

**REFRESH NOTE:** A cross check between this document and the proposed new version has been undertaken and all the requirements listed here are incorporated in the proposed new version.

The Panel will:

- Act as the principal non-executive, advisory function supporting those charged with governance;
- Be independent of the executive or operational responsibilities of the Mayor and Chief Constable;
- Have clear rights of access to other committees;
- Report to the GMCA Audit Committee on Police Fund activity and assurance;
- Be properly accountable to the Chief Constables’ Executive and GMCA Audit Committee (in relation to the Police Fund);
- Meet at least five times a year, and have a clear policy on those items to be considered in private and those to be considered in public;
- Be able to meet privately and separately with the external auditor and with the head of internal audit (outside of formal, public meetings);
- Include, as regular attendees, the chief financial officer(s) or appropriate senior and qualified substitute, the Chief Constable, the Chief Executive to GMCA, the head of internal audit and the appointed external auditor;
- Have the right to call, as required, any other GMP police officers/staff, GMCA officers, including the Mayor/Deputy Mayor;
- Report regularly on their work, and at least annually report an assessment of their performance.

**MEMBERSHIP**

The Panel will comprise a maximum of five members including the Chair who are independent of the Chief Constable and the Mayor. The meeting will only be quorate if at least three members are in attendance.

Initial term of office to be 3 years with up to a further 3 years on renewal.
Chair to be agreed by the Chief Constable/Mayor after considering applications for those interested.

SKILLS

To aid the Committee in delivering its purpose all Members will be required to undergo appropriate training which will be funded by the authority.

REVIEW

The Committee will review its terms of reference annually.
This page is intentionally left blank
Overview:

The purpose of this report is to inform Members of the Joint Audit Panel of progress to date regarding the review of strategic risk management arrangements in GMP.

The previous report, presented on 10 April 2019, gave detail of a new forward plan that was underway in GMP. This was to involve work with branch heads to develop assurance statements and collect branch risks. An update was presented on 15 January 2020 on the proposed new strategic risks.

Detail:

In early 2019, consultation and training was undertaken with branch heads to develop risk assurance statements for 14 branches/areas of work. These statements, signed off by branch heads, describe the risks that they manage on behalf of the Force and outline the governance structures they have in place to manage those risks, for example: management meetings, training plans, policies and procedures, contingencies, action plans or any external controls.

In April 2019, branch heads were also requested to highlight any key risks that they were managing that they felt required further debate at chief officer level, based on their professional judgement about their branch’s ability to control and mitigate those risks. Chief officers then convened for a quarterly risk management workshop. There was discussion about risk assurance statements and risks escalated by branches, and key strategic risk themes were agreed.

During May and June 2019, a series of meetings were held with DCC Pilling and ACO Potts to discuss plans for updating the Strategic Risk Register and alignment of the new risk management process with the Force Management Statement work programme. Two key decisions were made following these meetings: that the scope of the risk management work should be extended to (a) include the whole Force (districts in addition to branches) and (b) include the roll out of risk registers force-wide. Over the summer months, research took place to determine what this might look like. This included benchmarking with other forces/organisations. A series of options were presented back to chief officers for consideration.

In September 2019, a risk workshop took place involving the whole Force Leadership Team, at which all branch heads and territorial commanders were asked to consider the strategic risks in more detail and articulate the causes, impacts and mitigations in place.

A new Strategic Risk Register has been devised and is currently being reviewed by chief officers; however given the force’s response to the COVID-19 pandemic the final approval of the register will be delayed. A new risk register template for branches and districts, with associated scoring mechanism, risk definitions and guidance, has also been produced.
New Strategic Risk Register

The current Strategic Risk Register is shown at Appendix A and the proposed replacement at Appendix B. It has also been recently updated to include the risk of a pandemic.

The table below sets out the nine risks in the existing Strategic Risk Register and explains how these are reflected in the new proposed Strategic Risk Register, if applicable, or reasons for removal.

<table>
<thead>
<tr>
<th>Current Risk Register</th>
<th>Action Taken to add/remove from Proposed Risk Register</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policing Model Sustainability</td>
<td>Encapsulated within a number of risks on the new register (demand, local policing, finance, iOPs, representation, training, wellbeing)</td>
</tr>
<tr>
<td>Changing Policing Demands</td>
<td>Taken forward as SR1 on the new register</td>
</tr>
<tr>
<td>Representative Workforce</td>
<td>Taken forward as SR4 on the new register</td>
</tr>
<tr>
<td>SPR and Specialist Officers</td>
<td>Removed as now business as usual for Specialist Operations Branch</td>
</tr>
<tr>
<td>Resource Availability</td>
<td>Encapsulated within SR1 (demand management element) and SR5 (wellbeing element) on the new register</td>
</tr>
<tr>
<td>GM Governance</td>
<td>Removed as no longer a risk</td>
</tr>
<tr>
<td>Cohesion</td>
<td>Removed as now business as usual and managed via delivery plans</td>
</tr>
<tr>
<td>General Data Protection Regulation</td>
<td>Taken forward as SR8 on the new register</td>
</tr>
<tr>
<td>Transition to new iOPS/Police Works System</td>
<td>Taken forward as SR9 on the new register</td>
</tr>
</tbody>
</table>

The new register splits risks into three categories: operational risks, corporate risks, and information management / technology risks.

Forward Plan

It is proposed that 2020 will see a refresh of the risk assurance statements across all branches. This was intended to be an evolving process; the short term aim was to increase awareness, both individually for branch heads and collectively as a force, of the key risks that the organisation faces and be in a position to provide documented assurance that plans are in place to manage and escalate risks appropriately. Moving forward, the statements will be refined and made more consistent, with ‘live’ risks moved into new risk registers.
Risk registers are to be rolled out force-wide to branches and districts. The risk register template and scoring mechanism can be found at Appendix C. Support will be provided to branches and districts by External Relations and Performance Branch.

A review of branch and district risk registers will be presented to Operations Committee twice per year, allowing for the Strategic Risk Register to be updated twice per year at Executive Committee (the quarter following Operations Committee, so effectively strategic risks would be considered at force governance meetings on a quarterly basis).

The Force Risk Management Policy/Procedure will also be updated to reflect the new arrangements.
This page is intentionally left blank
Greater Manchester Police
Integrated Operational Policing System (iOPS)
An inspection to review the force’s action plan to reduce backlogs arising from the implementation of a new computer system
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Foreword</td>
<td>1</td>
</tr>
<tr>
<td>Introduction</td>
<td>2</td>
</tr>
<tr>
<td>Summary</td>
<td>5</td>
</tr>
<tr>
<td>Is the force fully aware of the volume and type of backlogs that have occurred?</td>
<td>8</td>
</tr>
<tr>
<td>Does the force understand the threat and risk in the backlogs and is it prioritising accordingly?</td>
<td>11</td>
</tr>
<tr>
<td>Does the force have a plan to reduce the backlogs and return GMP to its pre-iOPS level of demand?</td>
<td>14</td>
</tr>
<tr>
<td>Is the force effectively engaging with local partners and keeping them informed?</td>
<td>15</td>
</tr>
<tr>
<td>Does the force have a robust plan to support its officers and staff and build their confidence in iOPS?</td>
<td>16</td>
</tr>
<tr>
<td>Does the force have an effective plan in place to prevent further backlogs occurring?</td>
<td>18</td>
</tr>
<tr>
<td>Annex A: Elements of iOPS</td>
<td>20</td>
</tr>
</tbody>
</table>
Foreword

This inspection was conducted at the request of the Chief Constable of Greater Manchester Police (GMP) and commissioned by the Mayor’s Office of Greater Manchester Combined Authority. The terms of reference were set and agreed with HMICFRS under section 54(2BA) of the Police Act 1996.

This report is not a technical appraisal of the Integrated Operational Policing System (iOPS), GMP’s legacy systems nor its ICT infrastructure. Rather it is a review of the issues and operational difficulties that have become apparent since the launch of iOPS, and the response put in place.

The report includes the evidence and documents presented by the force at the time of inspection, supplemented by our own observations and the experiences of the staff we spoke to. This report does not include any evidence from GMP’s technical suppliers.

HMICFRS acknowledges the scale and complexity of the introduction of iOPS in GMP, and does not underestimate the challenges this presented. There is no doubt that some of the difficulties faced were unavoidable, however, different planning may have mitigated some of the issues encountered and there are obvious lessons to be learnt.

The reasons for the problems are similarly complex and multi-faceted. It is not our role to attribute specific cause nor responsibility. This is a matter for the force to resolve.

We are aware that since the completion of the inspection fieldwork, in November 2019, the force has continued to make progress in addressing some of the issues identified within this report.

Phil Gormley
HM Inspector of Constabulary
Introduction

About our inspection

Her Majesty’s Inspectorate of Constabulary and Fire and Rescue Services (HMICFRS) independently assesses and reports on the efficiency and effectiveness of police forces in England, Wales and Northern Ireland, in the public interest.

In July 2019, Greater Manchester Police (GMP) introduced a new computer system called the Integrated Operational Policing System\(^1\) (iOPS), originally scheduled to go live in March 2018. There have been significant problems with the performance of iOPS resulting in serious backlogs of work and a loss of staff confidence in the system. The problems with iOPS attracted negative media attention, in particular, concerning fears that public and officer safety were being put at risk.

The focus of the Mayor’s commission was for HMICFRS to review and assess the GMP recovery plan to remove the backlogs and restore staff and public confidence in iOPS.

Background

In 2019, GMP simultaneously replaced three ICT systems critical to how the force functions. The first was the command and control system which logs calls from members of the public and tracks the deployment of officers. The second and third were record management systems, containing intelligence, criminal investigations, custody records and files for court cases. iOPS also introduced systems to improve the use of mobile technology and demand management data. All forces need these capabilities to function.

All three legacy systems were old and GMP identified risks both to the force and the public should the systems fail. The force also recognised that it needed to invest in ICT to equip it for modern-day policing and to provide its workforce with the tools to police in an efficient and effective way.

The force decided to replace the old systems with one integrated system, iOPS. This contains two elements, one to replace the command and control system, called ControlWorks, and one to replace the records management systems, called PoliceWorks.

\(^1\) See Annex A.
The force predicted the introduction of the new system would change the way it operated, resulting in a number of benefits and efficiencies including:

- providing better quality information to officers and managers;
- officers being able to work remotely from mobile devices;
- reducing the need for duplication across multiple systems; and
- better information sharing with partner organisations.

We have commented on the need for GMP to deliver these expected benefits in our most recent PEEL\textsuperscript{2} inspection report on GMP.

Changing strategic computer systems is a complex undertaking and the introduction of iOPS has been a long-term programme for the force. It has been subject to several delays because of technical problems, extending the start date from the original implementation planned for March 2018.

In July 2019, iOPS went live. A major factor in this decision was the serious risk that the old systems could fail. The process for the transition from the old ICT systems to the new iOPS system is referred to as the ‘cutover’. The first stage was to migrate the force data from the old ICT systems to a legacy data store, which is a copy of all force data. Then the new PoliceWorks systems would be populated with agreed information from the legacy data store and commence usage.

To support the cutover phase, the force implemented a governance structure and prepared contingencies in case any anticipated issues arose. It also put in place a team of specialists to react to problems as they happened.

Despite this, problems became worse than anticipated. Three principal issues, individually and in combination, adversely affected the workforce’s ability to operate iOPS. Technical issues with the force ICT systems and infrastructure; changes to operational and working practices; and the training provided to operate the system.

These resulted in a loss of confidence by staff, particularly in the PoliceWorks system, and reduced force performance.

**Terms of reference**

The terms of reference for this inspection were to review the recovery plan put in place by GMP to resolve the difficulties and backlogs created by the implementation of iOPS.

We were asked to examine these questions:

1. Is the force ‘sighted on’ (fully aware of) the volume and type of backlogs that have occurred?
2. Does the force understand the threat and risk in the backlogs and is it prioritising accordingly?

\textsuperscript{2} PEEL is HMICFRS’s annual assessment of police forces in England and Wales. Forces are assessed on their effectiveness, efficiency and legitimacy.
3. Does the force have a plan to reduce the backlogs and return GMP to its pre-iOPS ‘state’?

4. Is the force effectively engaging with external partners and keeping them informed?

5. Does the force have a robust plan to support its officers and staff and build their confidence in iOPS?

6. Does the force have an effective plan in place to prevent further backlogs occurring?

It was not within the scope of our inspection to review:

- the programme management preceding the introduction of iOPS; or
- the functionality of iOPS as an ICT system.

However, in order to assess the force’s ability to return to their pre-iOPS state, it is necessary to examine both the pre and post-iOPS position to understand why the backlogs occurred. The technical capability of the system and the ability and confidence of staff to operate it, is relevant to reducing the backlogs and preventing a reoccurrence.

**Methodology**

The inspection was conducted during October and November 2019. We collated and analysed all relevant documents, plans and data. Interviews and focus groups were held with key individuals, staff, partners, union and staff association representatives. Unannounced reality testing was undertaken at police stations and in departments to understand staff perspectives. We specifically focused our attention on aspects of the business particularly affected by iOPS:

- crime recording and investigation;
- incident recording and response;
- criminal justice processes;
- criminal intelligence;
- vulnerability; and
- staff and partner confidence.

We are grateful for the candour and contribution of all those we met and spoke to.
Summary

Is the force fully aware of the volume and type of backlogs that have occurred?

We refer to the amount of unresolved work the force is dealing with as its backlogs. As two examples, this could be a call from a member of the public who is still waiting for a police officer to speak to them, or a crime that is still being investigated.

Following the introduction of iOPS, the force saw a large increase in the backlogs it had across the organisation. These didn’t occur due to one particular factor but were a combination of the complex and significant change both in its ICT and in its processes.

GMP is a complex organisation with high levels of demand and limited resources. The force’s ability to process this demand is based upon the productivity of its workforce; how much they can do during a working day. Critically, the introduction of iOPS lowered this productivity, creating a range of backlogs.

During the implementation of iOPS, difficulties meant the system didn’t work as effectively and efficiently as intended. The new systems also required staff to adopt new working practices. This combination of systems’ failure and unfamiliar processes substantially reduced organisational and individual productivity.

The force now understands the cause and volume of these backlogs. Data is being prepared on a live-time basis, which enables the organisation to identify and respond to backlogs.

Does the force understand the threat and risk in the backlogs and is it prioritising accordingly?

The force is prioritising action on most of the areas of high risk, but it doesn’t yet have a full understanding of the threat and risk that all the backlogs contain.

With the introduction of iOPS, the force changed the process for officers to submit referrals which ensure vulnerable people get the support they need. As a result, the number of referrals dramatically reduced.

Referrals to Greater Manchester Victims’ Services reduced by 87 percent. MARAC referrals for high-risk domestic abuse victims reduced by 50 percent. As part of Operation Alban and to better understand its demand, GMP conducted an internal audit which demonstrated that in one area, between 12–31 July 2019, only 28 percent of child protection incidents were referred to children’s social care.
The force has now put processes in place to quality assure these incidents and ensure the number of referrals returns to normal levels. However, at the time of our inspection, the force did not have a plan to backdate this or review unreferred incidents. Therefore, the force can’t be confident it has identified and appropriately referred all people at risk to partner agencies.

The call handlers and dispatch staff we spoke to, who deploy officers to incidents under a graded response process, were not trained in PoliceWorks. They need to be able to access and interrogate the system in order to properly understand information held and assess the risk presented by an incident. The force has recognised this problem and training for these staff was due to be completed by December 2019.

Even when staff have received training, users reported that searches on ControlWorks and PoliceWorks sometimes returned inconsistent or incorrect information about risks. We found examples where officers reported that they were unable to retrieve or readily access data when searching iOPS. In one domestic abuse incident involving a sexual offender, the risk had not been properly identified and it was graded as appropriate for telephone resolution. Unlike the old system, iOPS has no capability to search for different spellings of the same name, known as phonetic searching. This means the force can’t be sure that its officers and staff have all the known information available when they assess the level of risk and make operational decisions.

**Does the force have a plan to reduce the backlogs and return GMP to its pre-iOPS level of demand?**

In response to the increasing backlogs and in order to regain control, the force commenced Operation Alban. This has been led by the deputy chief constable, supported by a dedicated command structure, and involves shifting and abstracting resources from specialist branches from across the organisation to support tackling backlogs.

This will reduce the immediate backlogs but is diverting resources away from other important areas of work such as neighbourhood policing. It is not a sustainable long-term solution and has consequences for staff and service delivery, which the force recognises.

**Is the force effectively engaging with external partners and keeping them informed?**

The force was inconsistent in its engagement with external partners as part of the preparation and implementation of the iOPS programme. Some of the partners who operate at a force-wide level such as the Crown Prosecution Service (CPS) and court services were effectively communicated with. But engagement with local partners such as children’s and adults’ services was not as well structured or consistent.

The force is rectifying this and making sure that it effectively engages with all its external partners. Partners told us they were reassured by the force’s response to concerns and issues they had raised. The force has communicated with them at a strategic level to inform them of the backlogs and the action it is taking to address
the problems. This has resulted in staff from some partner organisations co-locating into police premises to support the ongoing work to reduce the backlogs.

**Does the force have a robust plan to support its officers and staff and build their confidence in iOPS?**

At the time of our inspection, we found that the force’s plan to support its officers and staff and build their confidence in iOPS was not sufficiently robust.

Many of the staff we spoke to still lack confidence in iOPS and the PoliceWorks system. In particular, problems with the system’s speed and functionality, coupled with issues regarding data quality and the ability to search systems, were major concerns. There were high levels of uncertainty regarding the ‘workarounds’ put in place to resolve some of these problems.

The force had identified this prior to the inspection and has tried to support its workforce and increase their confidence. This has included additional training, better communications and an increased number of ‘superusers’ able to support and help their colleagues.

However, officers and staff told us they felt they were being blamed for the backlogs occurring and were not being listened to when they raised concerns. They also told us that communications from the force and the chief officer team could have been better, both generally and in response to specific issues.

**Does the force have an effective plan in place to prevent further backlogs occurring?**

Preventing future backlogs will require a coherent plan to ensure issues which have contributed to the significant increase are prioritised and addressed. The force cannot continually commit resources to resolve these problems, as this will have consequences elsewhere.

The ability of the force to achieve a sustainable position is predicated on productivity returning to pre-iOPS levels. This requires:

- the force ICT system and infrastructure to function effectively;
- staff being trained and confident in the new ICT systems; and
- the adoption of new operational and working processes.

The force has taken some action to address these points. For example, it is working closely with the designers of the iOPS system to update it and resolve technical issues. However, at the time of our inspection, there was no overarching plan which assured us of its ability to prevent the recurrence of further backlogs.
Is the force fully aware of the volume and type of backlogs that have occurred?

Following the introduction of iOPS, the force saw a large increase in backlogs across the organisation, by which we mean the amount of unresolved demand the force still needs to work on. For example, this could be a call from a member of the public waiting for a police officer to speak to them, or a crime that is still being investigated.

The force anticipated some backlogs would be generated during the initial transfer, or ‘cutover’, for them to plateau and then return towards the pre-iOPS ‘business as usual’ levels. This did not happen, and problems continued, resulting in further increases to backlogs. They soon became unmanageable within the normal operating model and the resource levels available to the force.

The most significant backlogs identified by the force were:
- unresourced incidents in the control room;
- time taken for to answer 999 telephone calls;
- the number of ongoing criminal investigations; and
- the number of intelligence submissions awaiting assessment and evaluation.

Simultaneously, the force experienced large reductions in other important areas:
- referrals to victims’ services;
- MARAC referrals for high-risk domestic abuse victims; and
- successful electronic transfer of prosecution papers to the CPS.

The force identified these prior to our inspection and, in general, it has a good understanding of the volume and type of backlogs which have occurred since it launched iOPS.

These were generated by a combination of factors and were the result of the complex and significant change in both the force ICT systems and in its operational and working processes. GMP as an organisation receives a high level of demand and has limited resources. In general terms, the introduction of iOPS contributed to a reduction in the organisation’s productivity and its ability to process work through the system. This meant that incoming demand exceeded the amount being resolved, creating backlogs.
Some of the issues which contributed to this were a consequence of the challenging exercise to migrate legacy data into a new system. For example, fully understanding and mitigating the process changes within the PoliceWorks system for the multitude of tasks that were generated when several thousands of legacy investigations were moved across to the new system.

The initial transfer to iOPS generated an inevitable and unavoidable backlog. The force’s main ICT systems were shut down for 72 hours and replaced by paper records while the existing digital records migrated to iOPS. These paper records created during the migration period then needed to be back record converted onto iOPS. This consumed considerable time and capacity causing a duplication of work. In addition, some legacy demand which included ongoing investigations, did not successfully transfer from the old systems, so could no longer be worked on.

During implementation, the custody applications and systems failed. This meant that the force had to move to its contingency plans and use paper records. As a result, it was unable to transfer prosecution files electronically to the CPS. This again created duplication of effort.

Following the implementation, three principal issues, either individually or in combination, adversely affected the workforce’s ability to operate iOPS. These were:

- technical problems with force ICT systems and existing infrastructure;
- necessary changes to working practices; and
- the training provided to operate the PoliceWorks element of iOPS.

The problems faced by staff mainly related to the speed with which they could access the system and that it was unavailable for periods of time. On occasions, staff experienced long delays, in some cases waiting over 30 minutes for the PoliceWorks system to load. The introduction of iOPS required many systems of work to be changed and some of these, such as recording crime, searching records and making victim referrals, now take longer. Some of these changes to systems of work were planned and foreseen, others were contingencies put in place to mitigate problems which emerged following the transition to iOPS.

Training a workforce of 10,000 is a major undertaking, further complicated by the postponed implementation of iOPS. This meant most staff received training many months prior to the system going live and by the time iOPS was implemented, had lost knowledge and confidence in the system. Refresher training was delivered to mitigate the impact of the delays, but staff reported it as ineffective. The training primarily focused on technical aspects of iOPS, not the changed methods of working and new operational practices demanded for its introduction. In short, staff told us they felt ill prepared for the changes necessitated by iOPS.

At the time of our inspection, the iOPS systems had been operational for four months. During this period, backlogs were emerging and being discovered. For example, in the week prior to our inspection, the force identified 604 legacy crimes which hadn’t migrated to the new system. It reviewed the crimes and identified that most had either been investigated and required filing or had been allocated for investigation. However, 74 crimes – some of which were serious or complex involving vulnerable
victims – had not been allocated. The force told us it has reviewed each of these crimes to ensure appropriate investigations and proper support for the victims.

It was beyond the scope of our inspection to comment in detail on the effectiveness of the transfer or availability of information held on legacy systems.
Does the force understand the threat and risk in the backlogs and is it prioritising accordingly?

The force is prioritising action on most of the areas of high risk, but it doesn’t yet have a full understanding of the nature of the threat and risk that all the backlogs contain.

As the force developed its understanding of the backlogs, it began to identify and prioritise those containing the most threat and risk, such as incidents involving vulnerable people. However, this took time to achieve, meaning it exposed these vulnerable people to potential risk of harm.

The number of referrals the force made to partner agencies significantly reduced. This was caused by the change to PoliceWorks which, unlike the old system, does not have an automated process. This change had not been effectively communicated to operational staff. As a result, the force didn’t know if officers were generating the referrals and could not be sure it understood the level of threat and risk.

It took three months for the force to introduce a business process to quality assure that referrals were being made for child protection or domestic abuse incidents. Safeguarding units began to complete a daily search to identify and assess those which had not resulted in a referral. However, this was not completed retrospectively and, at the time of inspection, we were told that the force had no plans to do so. This may have prevented vulnerable people receiving the help they need. For example, an audit of backlogs in one district found that from 12–31 July 2019, only 28 percent of child protection incidents resulted in a referral. This is significantly lower than would normally be expected.

A similar process was also needed to address requests under the Domestic Violence Disclosure Scheme (DVDS). The changes brought about by iOPS meant that 137 requests under DVDS went unaddressed for three months. Once identified, this backlog was prioritised by the force and resources allocated to reduce it.

When officers attend a domestic abuse incident, they should assess the level of risk and complete a referral. Following the introduction of iOPS, the number of high-risk domestic abuse referrals to MARAC reduced by more than 50 percent in many districts across the force. There were also 686 domestic abuse incidents which had not been risk assessed, in some cases for over 100 days. Once the force identified this, it commenced reviewing these cases. Until it has completed the review, it can’t be sure it has identified the risk and made the appropriate referrals.
The introduction of iOPS changed the way in which victims of crime were referred to victims’ services. The changes made the process more complicated and as a result, these referrals reduced by 87 percent. The force has subsequently adapted the process to remedy this. However, it has no plans to review those crimes that weren’t referred at the time of report, meaning a number of victims may not have received the support they need.

Operation Encompass is designed to provide safeguarding for children who have been present at domestic abuse incidents, by informing the school they attend at the earliest opportunity. The GMP referral template loaded into PoliceWorks does not have a field to record this information. This means the force has experienced difficulties and delays informing schools. This issue will be rectified by an enhancement to PoliceWorks, however until that time officers have been reminded to record the school details within a free text field.

There is a nationally agreed target that all police forces will answer 999 calls in under 10 seconds. This is because the police must assume that those ringing 999 are facing a life or death emergency. After the initial launch of iOPS, the time the force took to answer emergency 999 calls increased from 12 seconds to 48 seconds. This was due to the increased complexity when compared with their legacy command and control system, and unfamiliarity with iOPS. At the time of the inspection, the average time to answer a 999 call had improved to 22 seconds. However, this still fails to meet the national target.

Call handlers and dispatch staff, who deploy officers to incidents under a graded response process, were not trained in PoliceWorks. They told us they need to be able to access and interrogate the system in order to properly understand the information held and assess the risk presented by an incident. The force has recognised this problem and training for these staff was due to be completed by December 2019.

There are risks relating to the information on iOPS being hard to retrieve, inconsistent, or inaccurate. The system has no capability to search for different spellings of the same name, known as phonetic searching. This means that if an officer doesn’t know the spelling of someone’s name, they may potentially miss important risk information. The alternative is to search every possible spelling. Even when the spelling is correct, for complicated technical reasons, users report that the system will sometimes return different search results against the same search criteria. This requires urgent remedial action.

During the inspection, the staff we spoke to provided numerous examples of information, such as criminal history and historic incidents, that they were unable to find via iOPS. This information could have been missed if officers had not been able to research the old ICT database. Consequently, they were concerned that their assessment of risk might have been adversely affected.

Examples included a domestic abuse incident involving a high-risk sex offender. This information wasn’t visible to the officer searching on PoliceWorks and the incident had been sent for resolution over the telephone. Also, a domestic abuse victim who had over 100 domestic abuse incidents linked to their record, was not visible on PoliceWorks. In both examples the information was clearly visible on the old ICT system. These and other examples have had a significant impact on officer
confidence that the quality of the information returned from a search is accurate. The force cannot be confident that its officers and staff have all the known information visible to them when they are making important operational decisions.

**Recommendation**

The force needs to develop a full understanding of the threat and risk contained within all its backlogs. In particular, it should review all domestic abuse incidents recorded by the force between the launch of iOPS and October 2019 to ensure that an appropriate response has been provided and referral made to the relevant agency.

**Recommendation**

The force should satisfy itself that all districts have completed a full audit of child protection incidents which occurred between the introduction of iOPS and the implementation of a quality assurance process which commenced in October 2019, to ensure appropriate referrals to partner agencies have been made.

**Recommendation**

The force should take steps to enhance the search capability within iOPS to ensure that the facility for the system to search for different spellings of the same name (phonetic searching) is available at the earliest opportunity.

**Recommendation**

The force should review those cases where victims of crime were not referred to victims’ services following the introduction of iOPS to ensure that any vulnerable victims receive appropriate support.

**Recommendation**

The force should ensure that all necessary data previously available on the legacy systems is easily searchable and accessible to officers and staff.
Does the force have a plan to reduce the backlogs and return GMP to its pre-iOPS level of demand?

The force does have a plan to reduce the backlogs and return to its pre-iOPS state. Because of the unmanageable backlogs the force was experiencing, it commenced Operation Alban to tackle them and keep the public safe.

This has been led by the deputy chief constable, supported by a dedicated command structure, and involves shifting and abstracting resources from across the organisation. It has seven key areas of focus and each of these has a strategic lead.

This plan will reduce the immediate backlogs, but it relies on resources being diverted from other important areas of work such as neighbourhood policing, as well as the use of overtime and employing temporary agency staff.

This approach has other potentially serious consequences, including not meeting the national standards for the recording and classification of crime, and delays in allocating criminal investigations. The intensification of work and the additional hours may also impact on staff wellbeing. The force is aware of this and has developed a plan to support its workforce.

The force, its officers and staff have remained resolutely focused on reducing the backlogs in demand and this has had a positive effect. There remains some way to go to return to pre-iOPS levels but without such a co-ordinated and focused drive, the backlogs would not have reduced as significantly as they have. By the time we inspected the force there were tangible results, for example:

- unresourced incidents in the control room returned to pre-iOPS levels;
- time to answer 999 telephone calls reduced;
- ongoing criminal investigations reduced by 12 percent from their peak;
- intelligence submissions awaiting assessment reduced;
- electronic transfer of prosecution papers to the CPS is now 95 percent successful; and
- victims’ services referrals increased to 50 percent of their original level.

The force recognises that it still has some way to go to address all the backlogs and has planned some additional activities to reduce them. It is also trying to ensure it achieves the expected increase in efficiency using the new ICT.
Is the force effectively engaging with local partners and keeping them informed?

The force engaged inconsistently with its external partners during the preparation and planning for the implementation of iOPS. However, it has remedied this and is now working closely with all its partners and keeping them properly informed.

During the inspection, we spoke to affected partners. We found that for organisations operating at a force-wide level, such as the CPS and court services, there had been effective engagement prior to implementation, strategic impact assessments had been undertaken and contingency plans developed.

But for organisations and partnerships operating at a more local level, such as children’s and adult services, the engagement was not as consistent or well structured. The force could have prepared its local partners better for the anticipated delays and created contingency plans to mitigate foreseeable problems. Also, its engagement wasn't early enough.

This meant that local partners were not properly or sufficiently able to respond when problems started to materialise. One of the more serious problems was the reduction in safeguarding referrals and the risks created. This delayed the timely flow of information between the police and its partner organisations to support the assessment and safeguarding of vulnerable people and children.

We were pleased to find that, once the impact on vulnerability and the reductions in referrals had been identified, the force responded effectively. It engaged at a strategic level with its partners to inform them of the backlog in demand and the action the force was taking to address the issues. This has resulted in staff from some partner organisations co-locating into police premises to support efforts to resolve the problems.

But the force should have made all its partners aware that they may receive increased demand as a result of Operation Alban. Some told us that their workload unexpectedly increased as they were receiving ‘batches’ of safeguarding referrals, which they then needed to review. A lack of co-ordinated activity may simply transfer risk from one organisation to another.

**Recommendation**

The force needs to ensure it effectively engages with partners at force and local level when undertaking significant change programmes.
Does the force have a robust plan to support its officers and staff and build their confidence in iOPS?

While the force has tried to support its workforce to improve confidence in the PoliceWorks element of iOPS, this support does not resolve the fundamental issues which staff regard as preventing them from effectively doing their jobs. In contrast, the ControlWorks system has had a greater degree of acceptance by staff. We found that staff confidence with this system is high.

During the inspection, we found staff motivated to do a good job with a real desire to keep people safe. However, they remain frustrated with the PoliceWorks system. They were clear regarding the problems presented by PoliceWorks and its significant impact on their efficiency and confidence. They articulated the following unresolved concerns with the system:

- logon time and the speed of the system when returning information;
- the inconsistency or accuracy of migrated historical data from previous force ICT systems;
- the need for greater functionality or range of options within the search facility;
- the ability of the search facility to return accurate results so that users do not have to search legacy systems; and
- confusion in the processes they are expected to follow, with changes to system ‘workarounds’ and frequent updates which they have found difficult to keep up with.

Officers and staff need to be confident that the data they can access is accurate and contains all the information they require to make effective decisions and assess levels of risk to support them to do their job. We have heard many examples from officers and staff who have experienced inaccuracies and missing data which they fear could have a significant impact on the safety of the public.

Officers also need to be confident in their ability to use the system. Due to iOPS being delayed, training for some staff was delivered many months prior to the implementation. Refresher training was provided but we were told this was ineffective and did not provide them with the skills and information they needed.

The force informed us of the post-implementation activities which it has put in place to support its officers and staff. These activities included: additional ‘superusers’ (people who have received additional training to help them to provide guidance and
support to colleagues within the operational environment); refresher training opportunities; drop in clinics to provide workload management advice and support; and information updates emailed to all staff. The force has also arranged workshops to better understand the concerns of its staff, such as the prevalence of inaccurate search information.

However, staff told us that they did not necessarily have time to access this support due to the levels of operational demand and the focus on reducing backlogs. The force should ensure that all staff receive additional training or support appropriate to their role.

The force may also wish to review their workforce communication strategy. Staff felt that communications from the force and the chief officer team had not been effective, both generally and in response to specific issues. They told us they felt at times they were being blamed for the increased demand and expected to trust a system in which they have very little confidence.

It is apparent that during implementation of the iOPS system, staff were reporting significant problems. Staff believe they weren’t listened to and lack confidence that their concerns were being addressed by the force. Numerous officers gave examples of issues raised with the helpdesk that had not been acknowledged or dealt with.

The force needs to develop a more effective communication and engagement plan and apply sufficient resource to deliver it. This should demonstrate to staff that it is listening to their feedback. It should provide clear communication that concerns have been heard and that the most significant issues are being prioritised and addressed. It needs to show how it intends to rectify the problems, and how it plans to improve confidence and user experience of PoliceWorks.

**Recommendation**

The force should review its internal communication plan to ensure all staff are informed, consulted and engaged in the ongoing development of iOPS.

**Recommendation**

The force should review and evaluate the operational effectiveness of its training plan for iOPS to ensure all staff are appropriately trained to enable them to carry out their role.
Does the force have an effective plan in place to prevent further backlogs occurring?

The force has improved management information and can use this to prevent backlogs from building. By using the PoliceWorks dashboard within iOPS for force data and management information, the force is now better equipped to identify and analyse its demand. The dashboard provides detailed live-time management information, which can be viewed by everyone in the force to monitor and keep up to date with outstanding demand. This includes overall incidents and vulnerability demand such as domestic abuse and missing people. The availability of this information enables the force to monitor and react to ongoing backlogs more quickly.

However, sustainably preventing future backlogs will require a coherent plan to ensure issues which have contributed to the significant increase are prioritised and addressed. The force cannot continually commit resources to resolve these problems, as this will have significant consequences elsewhere.

The ability of the force to achieve a sustainable position is predicated on productivity returning to pre-iOPS levels. The key factors affecting this are:

- the capability of the force ICT systems and infrastructure to function effectively;
- staff being trained and confident in new ICT systems; and
- the adoption of new operational and working processes.

The force has put measures in place to prevent backlogs reoccurring in some areas of policing. For example, scheduled updates are being agreed with the ICT provider to address some of the issues identified and improve how the system works. One system upgrade occurred during our inspection and more are planned for January 2020.

But for other issues that contributed to the backlogs and to the workforce’s lack of confidence in the system, plans are less clear. The force now needs to develop a comprehensive plan which addresses the key factors identified above. Critically, officers and staff need to have an understanding of the changes, and know what is expected of them. If the force is able to achieve this, then it has the potential to realise the operational and cultural benefits iOPS was intended to deliver.
Recommendation

The force should develop a sustainable approach to address the underlying problems with systems capability, training and the new operational and working processes.
Annex A: Elements of iOPS

The new Integrated Operational Policing System (iOPS) has four elements included within the programme of change. iOPS includes PoliceWorks, ControlWorks, Cognos and Mobile:

**PoliceWorks**

The iOPS PoliceWorks Records Management System covers a broad spectrum of police records. It includes crimes, investigations, custody, case preparation, prosecutions and appeal, managing the workflows of each event type and guiding users through the process.

It includes dashboards which provide users with access to their workload, summaries of data at a high level, and the ability to explore this in more detail and update individual records.

It allows GMP to gather and report on data that is accepted by the Police National Database (PND) and allows for searches against the Person, Object, Location and Event (POLE) criteria.

PoliceWorks can also integrate with national systems including Libra, the Police National Computer (PNC) and PND, as well as other third-party solutions, giving access to critical information. The PoliceWorks solution is designed to support the ‘digital first’ concept, removing the need for paper case files.

**ControlWorks**

iOPS ControlWorks is the new command and control system primarily used by the force Operational Communications Branch (OCB) officers and staff.

Benefits of ControlWorks include:

- Mapping: an active part of ControlWorks, mapping allows users to see exactly where people are in relation to incidents. It can also suggest the right resource to deploy based on response times, which should enable GMP to improve its service to the public.
- User friendly: there are several screens that display information, such as basic layout, incidents and maps.
- Promotes collaboration: maximises collaboration between other emergency responders and partner agencies.
Cognos

Cognos is the force data and management information solution that will help GMP monitor demand on each division, district or department. It will also assist it in strategic planning, by identifying longer-term trends.

An important feature of Cognos is to help GMP identify data quality issues, to ensure operational and performance data are accurate.

Mobile

All frontline operational staff received a new mobile device between Quarter 4 2019 and Quarter 1 2020. GMP invested in the Samsung S9 which meant that not only can all current applications be used on a much faster device, but also, the force can develop and deploy new apps to support operational police work.

As crime and communities change, the force needs reliable technology that will keep pace with the modern world.

Some of the new applications that will be introduced over time are:

- PDF scanners;
- QR Code readers and Digital Access to Forms which will make administrative tasks quicker; and
- Mobile Fingerprint Suspect Biometrics allowing fingerprints to be obtained and searched against the Live Scan and Immigration databases.
Joint GMP & GMCA overarching Anti-Fraud, Bribery and Corruption Policy and Procedure.

Update for the Joint Audit Panel on 8th April 2020.

Det. Supt Smith has been asked to lead on the development of the Anti-Fraud, Bribery and Corruption Policy and Procedure.

A draft Anti-Fraud, Bribery and Corruption Policy and Procedure has been produced following meetings with Sarah Horseman and Catherine Folan of the GMCA, DS Mark Smith and DCI Ged Scales of GMP Anti-Corruption Unit.

The overarching draft policy is supported by a number of existing draft GMP and GMCA policies, which have been included and referred to in paragraph 1.8.

The draft policy and procedure document is attached for consideration of the Joint Audit Panel members. If required, all other supporting policies and procedures referred to are available for consideration in conjunction with the draft policy. Subject to the observations, recommendations and required amendments from panel members, it is anticipated that the policy will be ready for final approval before the next panel meeting on the 29th June 2020.

Mark Smith,
Detective Superintendent,
Anti-Corruption Unit.
Overview:

The purpose of this progress report is to inform Members of the Joint Audit Panel of the progress to date of the delivery of the Internal Audit Plan.

Detail:

2018/20 Internal Audit Plan

The Internal Audit plan for 2018/20 was approved by the GM Mayor (in respect of police and crime functions), the Chief Constable and the Joint Audit Panel on 12th December 2018.

The plan contained 930 days of internal audit work. An additional 60 days were approved in April and June 2019 for inclusion in the plan. Based on a team of three auditors this plan contained more days than available resources for the period January 2019 - March 2020 therefore a revised audit plan was agreed by Force management and the Joint Audit Panel on 23rd October 2019.

Covid-19 impact on the Internal Audit Plan

The current Covid-19 pandemic is significantly impacting all aspects of delivery of the Internal Audit plan:

GMP

Understandably there has been an enormous impact on all staff within GMP during this national emergency. In consultation with the Head of Audit and Assurance the Treasurer of GMCA agreed that internal audit fieldwork be paused with effect from 19 March 2020 so as to allow GMP management and operational staff to focus on business continuity activity. Internal Audit resource has been offered to both GMP and GMCA to support business critical activity.

Internal Audit Team

Following government guidance, with effect from 23 March 2020 the internal audit team started to work from home. Internal Audit are not classed as key workers and therefore after the closure of all UK schools on 20th March 2020 two members of the internal audit team also have childcare responsibilities to manage. This includes the Head of Audit and Assurance. The team are working flexibly to accommodate new working arrangements. Whilst internal audit fieldwork is paused, the team will continue to progress any audit work ‘remotely’ they are able to, such as reporting
planning for future audits as well as reviewing and refreshing internal audit procedural documentation.

This progress report takes into consideration the current situation.

**Internal Audit Progress Update**

During quarter 4 we have been undertaking work in the following areas

Planning and Scoping (now paused):
- Forensic Digital Investigations
- Firearms Procurement

Fieldwork (now paused):
- Force Armoury
- Firearms Licensing
- PACE (Police and Criminal Evidence) Beds/Secure Beds for Juveniles Detention

Reporting stage (with Internal Audit)
- PCC Grants Process
- Crime Recording
- Compliance with Disclosure Responsibilities
- Human Tissue Act

Reporting stage (with GMP):
- Provision of Training – ‘newly promoted’ or ‘acting up’
- Detective Training - Initial Crime Investigators Development Programme
- Care and Family Services – Disclosure

Details of our progress in respect of the revised 2018/20 Audit Plan is shown in Appendix B.

**Changes to the Internal Audit Plan**

The internal audit plan is regularly reviewed and can be amended to reflect changing risks and/or objectives. In line with the Internal Audit Charter, significant changes to the plan must be approved by the Joint Audit Panel.

Given the current situation, it will not be possible to complete further audit work in the current financial year 2019/20. It is requested that the Panel approve that the audits in the remainder of the current plan are considered within the risk-based audit planning process for the 2020/21 Internal Audit plan.

Appendix C of this report provides a cumulative record of changes to the approved plan along with the date they were approved by the Panel.
Risk:

<table>
<thead>
<tr>
<th>Risk</th>
<th>Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual reports have identified risks associated with the area’s</td>
<td>Management has agreed to take appropriate action to address the issues</td>
</tr>
<tr>
<td>reviewed</td>
<td>identified and mitigate the associated risk.</td>
</tr>
</tbody>
</table>

Recommendations:

Members are asked to **review and scrutinise** the contents of this report.

Attachments:

Appendix A – Summary of internal audit reports 2019/20
Appendix B – 2018/20 Internal Audit Plan Progress Report
Appendix C – Record of Changes to the Internal Audit Plan
### 2019/20 Summary of Internal Audit Reports

The table below provides a cumulative summary of the internal audit work completed in 2019/20. This will inform the annual Internal Audit opinion for the year 2019/20.

<table>
<thead>
<tr>
<th>Audit</th>
<th>Assurance Level</th>
<th>Audit Actions</th>
<th>Summary of Critical/High Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Force Travel Desk</td>
<td>High</td>
<td>-</td>
<td>1 N/A</td>
</tr>
<tr>
<td>Mobile Working</td>
<td>Satisfactory</td>
<td>-</td>
<td>4 1 N/A</td>
</tr>
<tr>
<td>Uniform and Equipment</td>
<td>Satisfactory</td>
<td>-</td>
<td>1 5 2</td>
</tr>
<tr>
<td>Health and Safety</td>
<td>Satisfactory</td>
<td>-</td>
<td>7 4 N/A</td>
</tr>
<tr>
<td>Service Desk</td>
<td>High</td>
<td>-</td>
<td>2 - N/A</td>
</tr>
<tr>
<td>Force Assurance Arrangements for compliance with the Protection of Freedoms Act (2012)</td>
<td>Good</td>
<td>-</td>
<td>1 - N/A</td>
</tr>
<tr>
<td>GMP/GMSS Payroll 2018/19</td>
<td>Satisfactory</td>
<td>-</td>
<td>2 4 6</td>
</tr>
</tbody>
</table>

- The Uniform and Equipment ‘Entitlement List’ does not correspond with the items in the inventory. This could result in confusion when ordering items, that is, obsolete items being ordered or delays in processing orders.
- The number of overpayments to existing employees and leaving employees has increased since last year. Common themes for the overpayments are late notification to the GMSS team, which result in overpayment of leave and basic pay etc., and changes in working hours/patterns that have not been notified to
Audit testing found that a large percentage of notifications during the period December 2018 and January 2019, (42%) were received in the month of leaving or after the person had left. Subsequently an invoice has had to be raised to recover the overpayments.

<table>
<thead>
<tr>
<th>Service Area</th>
<th>Grade</th>
<th>Score</th>
<th>Risk</th>
<th>Impact</th>
<th>Compensation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Asset Management</td>
<td>Satisfactory</td>
<td>-</td>
<td>-</td>
<td>8</td>
<td>-</td>
</tr>
<tr>
<td>Specialist Equipment (Serious Crime Division)</td>
<td>Good</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>Custody Health and Welfare of Detainees</td>
<td>Good</td>
<td>-</td>
<td>-</td>
<td>1</td>
<td>4</td>
</tr>
<tr>
<td>Event Planning: Cost Recovery</td>
<td>Good</td>
<td>-</td>
<td>-</td>
<td>2</td>
<td>5</td>
</tr>
<tr>
<td>Cyber Security</td>
<td>Limited</td>
<td>-</td>
<td>6</td>
<td>9</td>
<td>1</td>
</tr>
</tbody>
</table>

1. IT security policies are in the process of being reviewed as they have not been updated for some time. For example, the latest version of the Appropriate Use of Electronic Communications and Information Systems is dated 17 February 2015. There are also some areas where there is no existing policy e.g. access control, incident reporting.
In addition, there is no policy or guidance available to inform users of their responsibilities regarding the reporting of potential security incidents as it is understood that users would contact the service desk if a security incident is suspected.

2. Whilst there are contract management arrangements in place, further work may be required to ensure due diligence checks and contract monitoring is sufficient in terms of cybersecurity risk.

3. Vulnerability scans are carried out as part of GMP’s annual IT Health Check. However, vulnerability scanning is not carried out in the intervening period.
   - GMP are looking to carry out a phishing email test to determine the number of individuals who may be vulnerable to this form of attack.
   - There are number of legacy operating systems and applications still in use.
   - There is no facility to place devices which have not been connected to the network in quarantine before they receive patches/updates.

4. There is no intrusion prevention system in operation.
   - The NCSC’s (National Cyber Security Centre) Domain Name Server (DNS) check (prevents access to domains known to be malicious)
cannot be utilised at present due to the network configuration.

There is currently no DDOS (Distributed Denial of Service) protection in place in respect of the GMP website.

5. Security monitoring requirements have not been formally defined, in terms of identifying types of events and activities that should be monitored.

6. Some security incidents including phishing emails and the DDOS occurring in 2018 are not recorded in the incident log.

- Phishing emails are not categorised as security incidents therefore details are not readily available.
- There is no specific procedural documentation held within IT in relation to the handling of specific IT cyber security related threats.

| Use of Agency Staff and Overtime (Serious Crime Division and Specialist Operations) | Limited | - | - | 7 | 2 | N/A |
| RIDDOR Accident Reporting | Limited | - | - | 4 | 3 | N/A |
### 2018/20 Internal Audit Plan Progress Report

The table below shows progress made in delivery of the 2018/20 Internal Audit Plan.

Key: ○ Not Yet started  ☐ Scheduled  ☐ In progress  ● Complete

<table>
<thead>
<tr>
<th>Assurance Theme</th>
<th>Auditable Area</th>
<th>Days</th>
<th>Timing</th>
<th>Scoping</th>
<th>Fieldwork</th>
<th>Draft Report</th>
<th>Final Report</th>
<th>Joint Audit Panel</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>Risk Management</td>
<td>20</td>
<td>Q4</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RIDDOR Reporting</td>
<td>10</td>
<td>Q2/3</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>Report Issued on 07.01.20</td>
</tr>
<tr>
<td>Workforce and People</td>
<td>Health and Safety</td>
<td>25</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>Report Issued on 25.03.19</td>
</tr>
<tr>
<td></td>
<td>Provision of Training – ‘newly promoted’ or ‘acting up’</td>
<td>10</td>
<td>Q1</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>Draft report sent to the Force on 11.11.19</td>
</tr>
<tr>
<td></td>
<td>Specially Trained Officers</td>
<td>15</td>
<td>Q2/3</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>Draft report sent to the Force on 10.02.20</td>
</tr>
<tr>
<td>Assets and Equipment</td>
<td>Uniform and Equipment – issue, returns, monitoring and reporting</td>
<td>20</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>Report Issued on 21.03.19</td>
</tr>
<tr>
<td></td>
<td>Management of Specialist Equipment within Serious Crime Division</td>
<td>20</td>
<td>Q1</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>Report Issued on 24.10.19</td>
</tr>
<tr>
<td></td>
<td>Firearms – security, issue and return to Force Armoury</td>
<td>10</td>
<td>Q3</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>FIELDWORK PAUSED</td>
</tr>
<tr>
<td></td>
<td>Firearms – physical control and storage of firearms held</td>
<td>20</td>
<td>Q4</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td></td>
</tr>
<tr>
<td>Assurance Theme</td>
<td>Auditable Area</td>
<td>Days</td>
<td>Timing</td>
<td>Scoping</td>
<td>Fieldwork</td>
<td>Draft Report</td>
<td>Final Report</td>
<td>Joint Audit Panel</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------------</td>
<td>----------------</td>
<td>------</td>
<td>--------</td>
<td>---------</td>
<td>-----------</td>
<td>--------------</td>
<td>--------------</td>
<td>-------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Procurement and Contracts</td>
<td>Firearms Procurement</td>
<td>15</td>
<td>Q4</td>
<td>⬜️</td>
<td>⬜️</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Procurement</td>
<td></td>
<td>25</td>
<td>Q4</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Information, Data Governance and Security</td>
<td>Force Assurance Arrangements for compliance with the Protection of Freedoms Act (Biometrics)</td>
<td>5</td>
<td>Q4</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
</tr>
<tr>
<td>Change and Transformation</td>
<td>Forensic Digital Investigations</td>
<td>20</td>
<td>Q4</td>
<td>⬜️</td>
<td>⬜️</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Firearms Regional Training Collaboration</td>
<td></td>
<td>15</td>
<td>Q4</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
</tr>
<tr>
<td>Finance</td>
<td>GMP Travel Desk (VFM)</td>
<td>10</td>
<td></td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
</tr>
<tr>
<td>CTPNW Travel Desk (VFM)</td>
<td></td>
<td>10</td>
<td></td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
</tr>
<tr>
<td>Payroll</td>
<td></td>
<td>30</td>
<td></td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
</tr>
<tr>
<td>Use of Agency Staff and Overtime (Serious Crime Division and Specialist Operations Branch)</td>
<td></td>
<td>20</td>
<td>2018/19</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
</tr>
<tr>
<td>Events Planning – Cost</td>
<td></td>
<td>25</td>
<td>Q1/2</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
<td>⬜️</td>
</tr>
<tr>
<td>Assurance Theme</td>
<td>Auditable Area</td>
<td>Days</td>
<td>Timing</td>
<td>Scoping</td>
<td>Fieldwork</td>
<td>Draft Report</td>
<td>Final Report</td>
<td>Joint Audit Panel</td>
<td>Comments</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>------</td>
<td>---------</td>
<td>---------</td>
<td>-----------</td>
<td>--------------</td>
<td>--------------</td>
<td>-------------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Recovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custody and Criminal Justice</td>
<td>Health and Welfare of Detainees in Custody and on Release</td>
<td>20</td>
<td>Q1/2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Disclosure - Compliance</td>
<td>25</td>
<td>Q1/2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Report Issued 30.10.19</td>
</tr>
<tr>
<td></td>
<td>PACE (Police and Criminal Evidence) Beds/Secure Beds for Juveniles</td>
<td>20</td>
<td>Q3/4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REPORTING (WITH IA)</td>
</tr>
<tr>
<td>Performance</td>
<td>Crime Recording</td>
<td>20</td>
<td>Q3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REPORTING (WITH IA)</td>
</tr>
<tr>
<td>ICT and Information Systems</td>
<td>Mobile Working</td>
<td>10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Report Issued 18.03.19</td>
</tr>
<tr>
<td></td>
<td>Service Management Platform – Service Desk</td>
<td>10</td>
<td>Q4 2018/19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Report Issued 06.06.19</td>
</tr>
<tr>
<td></td>
<td>Software Asset Management</td>
<td>10</td>
<td>Q4 2018/19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Report Issued 24.07.19</td>
</tr>
<tr>
<td></td>
<td>Cyber Security</td>
<td>15</td>
<td>Q1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Report Issued 02.12.19</td>
</tr>
<tr>
<td></td>
<td>CARE Family by Disclosure in Criminal Records</td>
<td>10</td>
<td>Q2/3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Draft report sent to the Force on 26.02.20</td>
</tr>
<tr>
<td></td>
<td>Human Tissue</td>
<td>5</td>
<td>Q4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>REPORTING (WITH IA)</td>
</tr>
<tr>
<td></td>
<td>GDPR – an audit of the processes in place to become</td>
<td>5</td>
<td>Q4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assurance Theme</td>
<td>Auditable Area</td>
<td>Days</td>
<td>Timing</td>
<td>Scoping</td>
<td>Fieldwork</td>
<td>Draft Report</td>
<td>Final Report</td>
<td>Joint Audit Panel</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------------------</td>
<td>----------------------------------------------</td>
<td>------</td>
<td>--------</td>
<td>---------</td>
<td>-----------</td>
<td>--------------</td>
<td>--------------</td>
<td>-------------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>and maintain GDPR compliance</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Follow up audits</td>
<td>Seized Cash and Proceeds of Crime</td>
<td>5</td>
<td></td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>Report Issued 28.01.19</td>
</tr>
<tr>
<td></td>
<td>Police and Crime Commissioning Framework</td>
<td>5</td>
<td>Q1</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>Covered in PCC Audit</td>
</tr>
<tr>
<td>Police and Crime Function</td>
<td>Audit Needs Assessment and Audits</td>
<td>5</td>
<td>Q2</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>●</td>
<td>ANA Exercise completed</td>
</tr>
<tr>
<td>Grants – Receipt, Allocation and Processing</td>
<td></td>
<td>30</td>
<td>Q4</td>
<td>●</td>
<td>●</td>
<td>○</td>
<td>○</td>
<td>○</td>
<td>REPORTING (WITH IA)</td>
</tr>
</tbody>
</table>
Changes to the Internal Audit Plan

The internal audit plan is designed to be flexible and can be amended to address changes in the risks and/or strategic objectives. Similarly management and the board may request additional audit work be performed to address particular issues. In line with Public Sector Internal Audit Standards (PSIAS) the Joint Audit Panel should approve any significant changes to the plan.

This Section records all changes to the internal audit plan.

<table>
<thead>
<tr>
<th>Assurance Theme</th>
<th>Auditable Area</th>
<th>Impact on Audit days</th>
<th>Change requested by</th>
<th>Rationale</th>
<th>Approved by Joint Audit Panel</th>
</tr>
</thead>
<tbody>
<tr>
<td>Governance</td>
<td>Risk Management</td>
<td>+20</td>
<td>Joint Audit Panel</td>
<td>Assurance on new arrangements</td>
<td>April 2019</td>
</tr>
<tr>
<td>Procurement</td>
<td>Procurement</td>
<td>+25</td>
<td>Joint Audit Panel</td>
<td>Assurance on current arrangements</td>
<td>April 2019</td>
</tr>
<tr>
<td>Workforce and People</td>
<td>RIDDOR Reporting</td>
<td>+10</td>
<td>Force – ACO Potts</td>
<td>Assurance on new system</td>
<td>June 2019</td>
</tr>
<tr>
<td>Assets and Equipment</td>
<td>Equipment – Fit for Purpose</td>
<td>-20</td>
<td>Head of Audit and Assurance</td>
<td>Re-cast of 2018/20 plan to align with available Internal Audit resource.</td>
<td>October 2019</td>
</tr>
<tr>
<td>Change and Transformation</td>
<td>Payroll HR Shared Service</td>
<td>-10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Change Management Process</td>
<td>-30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance</td>
<td>Governance and Decision Making</td>
<td>-25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Organisational Learning</td>
<td>-20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICT and Information systems</td>
<td>ICT Systems Health Checks</td>
<td>-5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service Integration and Management</td>
<td>-10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information, Data Governance and Security</td>
<td>Human Tissue Act</td>
<td>-5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>IS Requests for Information</td>
<td>-25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Category</td>
<td>Description</td>
<td>Priority</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mobile Digital Devices</td>
<td>-20</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS Sharing of Information</td>
<td>-25</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IS Incidents and Breaches</td>
<td>-25</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procurement and Contracts</td>
<td>Firearms Procurement</td>
<td>-15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Contract Management and Monitoring</td>
<td>-30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workforce and People</td>
<td>Provision of Training</td>
<td>-25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restricted Duties</td>
<td>-25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Follow up</td>
<td>Mail and Mailboxes</td>
<td>-5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PCC</td>
<td>Victims Services</td>
<td>-30</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information, Data Governance and Security</td>
<td>Human Tissue Act</td>
<td>+5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Governance</td>
<td>Risk Management</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Assets and equipment</td>
<td>Firearms – physical control and storage of firearms held across the Force e.g. in Forensics and Property Stores</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Procurement and contracts</td>
<td>Procurement</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Change and transformation</td>
<td>Firearms Regional Training Collaboration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ICT and information systems</td>
<td>GDPR – an audit of the processes in place to become GDPR compliant</td>
<td>5</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Head of Audit and Assurance**

- Request received from Force to schedule in Q4 2019/20
- Not possible to undertake the audit in 2019/20 due to Covid-19. Request the audit is considered for inclusion in the 2020/21 plan during the risk-based planning process
Overview:
The purpose of this report is to inform Members of the Joint Audit Panel of the progress made in developing the 2020/21 Internal Audit Plan.

Detail:
Internal Audit have commenced the risk-based planning process for the Internal Audit services to be provided to GMP/PCC for the year 2020/21 and beyond. Due to unforeseen changes in working arrangements arising from the Covid-19 pandemic which affects both the Internal Audit team and GMP, the planning process has temporarily been paused in order to allow GMP resources to focus on business critical activities.

This report provides the Panel with an update on the progress that has been made with the plan and the anticipated next steps when normal working arrangements resume.

Planning Approach
As previously presented to the Audit Panel the audit planning approach is as shown overleaf.
The green ticks/pauses on the diagram show the progress made in the planning process up to the middle of March 2020 with a brief outline of progress explained below.

**Step 1 – Understand Strategic Objectives and Risks**

The Standing Together Plan is a plan for the police, community safety, criminal justice services and citizens in Greater Manchester. The plan sets out the priorities, commitments and outcomes that have driven GMP/PCC’s and the wider GMCA’s work between 2018 and 2021. It also set the strategic direction for policing and community safety. The three key priorities were identified as helping make Greater Manchester one of the best places in the world to grow up, get on and grow old were identified as:

1. Keeping people safe
2. Reducing harm and offending
3. Strengthening communities and places
Within each of the priorities there are a number of commitments and outcomes identified that help shape the activities and focus of GMP/PCC and wider GMCA. Understanding these priorities and outcomes helps Internal Audit put into context the activities of GMP/PCC.

An updated strategic risk register has been developed by GMP. This was shared with Internal Audit at the beginning of March 2020. It is useful to understand the strategic risks faced by GMP and focus our internal audit work going forwards on the key areas of risk.

**Step 2 – Identify the Audit Universe**

The Audit Universe is a view of all the activities undertaken by GMP/PCC. The current Audit Universe has been drafted and agreed with the Deputy Chief Constable.

**Step 3 – Assess risks**

Each auditable unit is risk assessed. The assessment takes into consideration a number of factors, including:

- Whether the activity is deemed a **critical function**
- The **pervasiveness** of the activity (i.e. is it a forcewide activity, does it impact multiple-branches or is it a self contained activity)
- Does the activity impact **core policing** activity?
- If something went wrong within the activity, what is the degree of **reputational risk** to GMP/PCC
- Whether the activity impacts the **capital programme**
- What is the degree of risk to officers’, staff or public **health and safety**?
- Does the activity directly link to a **strategic priority/outcome** within the Standing Together Plan
- Whether the activity directly impacts one of the identified **Strategic Risks**.

An initial risk assessment has been undertaken by Internal Audit. It is however important at this stage to validate the risk assessment with the Force. It had been planned to attend the ExecCo meeting on 24 March 2020 to discuss the approach to validating the risk assessment and determining the resultant plan with GMP Leadership. However, understandably this meeting did not take place. The planning process has therefore paused at this stage.

**Step 4 – Determine Audit Frequency**

The audit frequency is determined by the risk assessment process. An initial view of audit frequency has been developed. This will be updated alongside the risk assessment validation exercise as Step 3 above.
Proposed Next Steps:

1. There are a number of audits that have been paused or not started in 2019/20 due to the Covid-19 situation. It is proposed initially to continue and complete those audits in order to effectively utilise Internal Audit resources as soon as working arrangements start to return to pre-Covid-19 arrangements.
2. When the situation eases and working arrangements become stable, Internal Audit will work with Force management to resume and complete the audit planning process.
3. If the Audit Panel would like Internal Audit to focus on any specific areas in the forthcoming plan, please communicate these to the Head of Internal Audit for inclusion into the plan.

Recommendations:

Members are asked to note the contents of this report.

Attachments:

N/A
CONTENTS

1. Engagement and responsibilities summary
2. Your audit engagement team
3. Audit scope, approach and timeline
4. Significant risks and key judgement areas
5. Value for Money
6. Fees for audit and other services
7. Our commitment to independence
8. Materiality and misstatements

Appendix A – Key communication points
Appendix B - Forthcoming accounting and other issues
Appendix C – Mazars’ client service commitment [optional]
Dear Sirs / Madams

Audit Strategy Memorandum – Year ending 31 March 2020

We are pleased to present our Audit Strategy Memorandum for the Chief Constable of Greater Manchester (the Chief Constable) for the year ending 31 March 2020.

The purpose of this document is to summarise our audit approach, highlight significant audit risks and areas of key judgements and provide you with the details of our audit team. As it is a fundamental requirement that an auditor is, and is seen to be, independent of its clients, Section 7 of this document also summarises our considerations and conclusions on our independence as auditors.

We consider two-way communication with you to be key to a successful audit and important in:

- reaching a mutual understanding of the scope of the audit and the responsibilities of each of us;
- sharing information to assist each of us to fulfil our respective responsibilities;
- providing you with constructive observations arising from the audit process; and
- ensuring that we, as external auditors, gain an understanding of your attitude and views in respect of the internal and external operational, financial, compliance and other risks facing the Chief Constable which may affect the audit, including the likelihood of those risks materialising and how they are monitored and managed.

This document, which has been prepared following our initial planning discussions with management, is the basis for discussion of our audit approach, and any questions or input you may have on our approach or role as auditor.

This document also contains specific appendices that outline our key communications with you during the course of the audit, and forthcoming accounting issues and other issues that may be of interest.

Client service is extremely important to us and we strive to continuously provide technical excellence with the highest level of service quality, together with continuous improvement to exceed your expectations so, if you have any concerns or comments about this document or audit approach, please contact me on 0113 394 5316.

Yours faithfully

Mark Dalton
Mazars LLP
Overview of engagement
We are appointed to perform the external audit of Chief Constable of Greater Manchester Police (GMP) for the year to 31 March 2020. The scope of our engagement is set out in the Statement of Responsibilities of Auditors and Audited Bodies, issued by Public Sector Audit Appointments Ltd (PSAA) available from the PSAA website: https://www.psaa.co.uk/audit-quality/statement-of-responsibilities/

Our responsibilities
Our responsibilities are principally derived from the Local Audit and Accountability Act 2014 (the 2014 Act) and the Code of Audit Practice issued by the National Audit Office (NAO), as outlined below:

Audit opinion
We are responsible for forming and expressing an opinion on the financial statements. Our audit is planned and performed so to provide reasonable assurance that the financial statements are free from material error and give a true and fair view of the financial performance and position of the Chief Constable for the year.

Value for Money
We are required to conclude whether the Chief Constable has proper arrangements in place to secure economy, efficiency and effectiveness in its use of resources. We discuss our approach to Value for Money work further in section 5 of this report.

Electors’ rights
The 2014 Act requires us to give an elector, or any representative of the elector, the opportunity to question us about the accounting records of the Chief Constable and consider any objection made to the accounts. We also have a broad range of reporting responsibilities and powers that are unique to the audit of local authorities in the United Kingdom.

Our audit does not relieve management or those charged with governance, of their responsibilities. The responsibility for safeguarding assets and for the prevention and detection of fraud, error and non-compliance with law or regulations rests with both those charged with governance and management. In accordance with International Standards on Auditing (UK), we plan and perform our audit so as to obtain reasonable assurance that the financial statements taken as a whole are free from material misstatement, whether caused by fraud or error. However our audit should not be relied upon to identify all such misstatements.

As part of our audit procedures in relation to fraud we are required to enquire of those charged with governance as to their knowledge of instances of fraud, the risk of fraud and their views on management controls that mitigate the fraud risks.

The Chief Constable is required to prepare its financial statements on a going concern basis by the Code of Practice on Local Authority Accounting. As auditors, we are required to consider the appropriateness of the use of the going concern assumption in the preparation of the financial statements and the adequacy of disclosures made.

For the purpose of our audit, we have identified the Joint Audit Panel as those charged with governance.
2. YOUR AUDIT ENGAGEMENT TEAM

- **Mark Dalton** – Director and Engagement Lead
  - E: Mark.Dalton@mazars.co.uk
  - T: 0113 394 5316 / 07795 506766

- **Alastair Newall, Senior Manager**
  - E: alastair.newall@mazars.co.uk
  - T: 0161 238 9243 / 07909 986776

- **Amelia Payton** – Assistant Manager
  - E: Amelia.Payton@mazars.co.uk
  - T: 0161 238 9308 / 07823 521012

In addition as outlined in our engagement pack an engagement quality control reviewer has been appointed for this engagement.
3. AUDIT SCOPE, APPROACH AND TIMELINE

Audit scope

Our audit approach is designed to provide an audit that complies with all professional requirements.

Our audit of the financial statements will be conducted in accordance with International Standards on Auditing (UK), relevant ethical and professional standards, our own audit approach and in accordance with the terms of our engagement. Our work is focused on those aspects of your business which we consider to have a higher risk of material misstatement, such as those affected by management judgement and estimation, application of new accounting standards, changes of accounting policy, changes to operations or areas which have been found to contain material errors in the past.

Audit approach

Our audit approach is a risk-based approach primarily driven by the risks we consider to result in a higher risk of material misstatement of the financial statements. Once we have completed our risk assessment, we develop our audit strategy and design audit procedures in response to this assessment.

If we conclude that appropriately-designed controls are in place then we may plan to test and rely upon these controls. If we decide controls are not appropriately designed, or we decide it would be more efficient to do so, we may take a wholly substantive approach to our audit testing. Substantive procedures are audit procedures designed to detect material misstatements at the assertion level and comprise tests of details (of classes of transactions, account balances, and disclosures) and substantive analytical procedures. Irrespective of the assessed risks of material misstatement, which take into account our evaluation of the operating effectiveness of controls, we are required to design and perform substantive procedures for each material class of transactions, account balance, and disclosure.

Our audit will be planned and performed so as to provide reasonable assurance that the financial statements are free from material misstatement and give a true and fair view. The concept of materiality and how we define a misstatement is explained in more detail in section 8.

The diagram below outlines the procedures we perform at the different stages of the audit.
Reliance on internal audit

Where possible we will seek to utilise the work performed by internal audit to modify the nature, extent and timing of our audit procedures. We will meet with internal audit to discuss the progress and findings of their work prior to the commencement of our controls evaluation procedures.

Where we intend to rely on the work of internal audit, we will evaluate the work performed by your internal audit team and perform our own audit procedures to determine its adequacy for our audit.

Management’s and our experts

Management makes use of experts in specific areas when preparing the Chief Constable’s financial statements. We also use experts to assist us to obtain sufficient appropriate audit evidence on specific items of account.

<table>
<thead>
<tr>
<th>Items of account</th>
<th>Management’s expert</th>
<th>Our expert</th>
</tr>
</thead>
<tbody>
<tr>
<td>Defined benefit liability</td>
<td>Actuaries: • Government Actuary’s Department(GAD) for police officers; and • Hyman Robertson for all other employees.</td>
<td>PwC, consulting actuary engaged by the National Audit Office</td>
</tr>
</tbody>
</table>

Service organisations

International Auditing Standards (UK) define service organisations as third party organisations that provide services to the Chief Constable that are part of its information systems relevant to financial reporting. We are required to obtain an understanding of the services provided by service organisations as well as evaluating the design and implementation of controls over those services. The table below summarises the service organisations used by the Chief Constable and our planned audit approach.

<table>
<thead>
<tr>
<th>Items of account</th>
<th>Service organisation</th>
<th>Audit approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Payroll</td>
<td>Trafford MBC</td>
<td>We plan to obtain assurance by understanding the processes and controls that the Chief Constable has in place to ensure that transactions are processed correctly. Our approach will also include sample testing of transactions.</td>
</tr>
<tr>
<td>Payment of pension lump sums and monthly pension payroll to retirees under the Police Pension schemes.</td>
<td>XPS</td>
<td>As above</td>
</tr>
</tbody>
</table>
4. SIGNIFICANT RISKS AND KEY JUDGEMENT AREAS

Following the risk assessment approach discussed in section 3 of this document, we have identified relevant risks to the audit of financial statements. The risks that we identify are categorised as significant, enhanced or standard, as defined below:

**Significant risk** A significant risk is an identified and assessed risk of material misstatement that, in the auditor’s judgment, requires special audit consideration. For any significant risk, the auditor shall obtain an understanding of the entity’s controls, including control activities relevant to that risk.

**Enhanced risk** An enhanced risk is an area of higher assessed risk of material misstatement at audit assertion level other than a significant risk. Enhanced risks incorporate but may not be limited to:

- key areas of management judgement, including accounting estimates which are material but are not considered to give rise to a significant risk of material misstatement; and
- other audit assertion risks arising from significant events or transactions that occurred during the period.

**Standard risk** This is related to relatively routine, non-complex transactions that tend to be subject to systematic processing and require little management judgement. Although it is considered that there is a risk of material misstatement, there are no elevated or special factors related to the nature, the likely magnitude of the potential misstatements or the likelihood of the risk occurring.

The summary risk assessment, illustrated in the table below, highlights those risks which we deem to be significant. We have summarised our audit response to these risks on the next page.
4. SIGNIFICANT RISKS AND KEY JUDGEMENT AREAS (CONTINUED)

We provide more detail on the identified risks and our testing approach with respect to significant risks in the table below. An audit is a dynamic process; should we change our view of risk or approach to address the identified risks during the course of our audit, we will report this to the Joint Audit Panel.

**Significant risks**

<table>
<thead>
<tr>
<th>Description of risk</th>
<th>Planned response</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1 Management override of controls</strong></td>
<td>We plan to address the management override of controls risk through performing audit work over accounting estimates, journal entries and significant transactions outside the normal course of business or otherwise unusual.</td>
</tr>
<tr>
<td>Management at various levels within an organisation are in a unique position to perpetrate fraud because of their ability to manipulate accounting records and prepare fraudulent financial statements by overriding controls that otherwise appear to be operating effectively. Due to the unpredictable way in which such override could occur there is a risk of material misstatement due to fraud on all audits.</td>
<td></td>
</tr>
<tr>
<td><strong>2 Defined benefit liability valuation</strong></td>
<td>In relation to the valuation of GMP’s defined benefit pension liability we will:</td>
</tr>
<tr>
<td>The net pension liability represents a material element of GMP’s balance sheet. GMP’s liability is split between the Greater Manchester Pension Scheme and the Police Pension Scheme. The valuation of the pension scheme liabilities relies on a number of assumptions, most notably around the actuarial assumptions, and actuarial methodology which results in GMP’s overall valuation. There are financial assumptions and demographic assumptions used in the calculation of GMP’s valuation, such as the discount rate, inflation rates and mortality rates. The assumptions should also reflect the profile of GMP’s employees, and should be based on appropriate data. The basis of the assumptions is derived on a consistent basis year to year, or updated to reflect any changes. There is a risk that the assumptions and methodology used in valuing GMP’s pension obligation are not reasonable or appropriate to GMP’s circumstances. This could have a material impact to the net pension liability in 2019/20.</td>
<td>• Critically assess the competency, objectivity and independence of the Greater Manchester Pension Fund’s Actuary, Hymans Robertson and the Police Pension Scheme Actuary, the Government Actuary Department (GAD); • Liaise with the auditors of the Greater Manchester Pension Fund to gain assurance that the controls in place at the Pension Fund are operating effectively. This will include the processes and controls in place to ensure data provided to the Actuary by the Pension Fund for the purposes of the IAS19 valuation is complete and accurate; • Review the appropriateness of the Pension Asset and Liability valuation methodologies applied by the Pension Fund Actuary, and the key assumptions included within the valuation. This will include comparing them to expected ranges, utilising information provided by PWC, consulting actuary engaged by the National Audit Office; • Agree the data in the IAS 19 valuation report provided by the Funds Actuaries for accounting purposes to the pension accounting entries and disclosures in GMP’s financial statements.</td>
</tr>
</tbody>
</table>

4. SIGNIFICANT RISKS AND KEY JUDGEMENT AREAS (CONTINUED)

Significant risks

Revenue recognition

International Standard on Auditing (ISA) 240 includes a rebuttable presumption that the fraud risk from revenue recognition is a significant audit risk.

We recognise that the nature of revenue in local government differs significantly to the sources of income in the private sector. We also consider that there are limited incentives and opportunities to manipulate the way income is recognised in local government.

Based on our understanding of the GMP’s revenue streams we have rebutted the presumption that revenue recognition is a significant risk at GMP. Our testing of revenue is focused on our standard procedures and does not incorporate specific work on the risk of fraud in recognising revenue.
5. VALUE FOR MONEY CONCLUSION

Our approach to the Value for Money conclusion

We are required to form a conclusion as to whether GMP has made proper arrangements for securing economy, efficiency and effectiveness in its use of resources. The NAO issues guidance to auditors that underpins the work we are required to carry out, and sets out the overall criterion and sub-criteria that we are required to consider.

The overall criterion is that, ‘in all significant respects, GMP had proper arrangements to ensure it took properly informed decisions and deployed resources to achieve planned and sustainable outcomes for taxpayers and local people.’

To assist auditors in reaching a conclusion on this overall criterion, the following sub-criteria are set out by the NAO:

- informed decision making;
- sustainable resource deployment; and
- working with partners and other third parties.

A summary of the work we undertake to reach our conclusion is provided below:

<table>
<thead>
<tr>
<th>Risk assessment</th>
<th>Risk mitigation work</th>
<th>Other procedures</th>
</tr>
</thead>
<tbody>
<tr>
<td>NAO Guidance</td>
<td>Planned procedures to mitigate the risk of forming an incorrect conclusion on arrangements</td>
<td>Consider the work of regulators</td>
</tr>
<tr>
<td>Sector-wide issues</td>
<td></td>
<td>Consider the Annual Governance Statement</td>
</tr>
<tr>
<td>Your operational and business risks</td>
<td></td>
<td>Consistency review and reality check</td>
</tr>
<tr>
<td>Knowledge from other audit work</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Significant Value for Money risks

The NAO’s guidance requires us to carry out work at the planning stage to identify whether or not a Value for Money (VFM) exists. Risk, in the context of our VFM work, is the risk that we come to an incorrect conclusion rather than the risk of the arrangements in place at GMP being inadequate. As outlined above, we draw on our deep understanding of GMP and its partners, the local and national economy and wider knowledge of the public sector.

For the 2019/20 financial year, we have set out below a significant risk to our VFM conclusion. In addition we have still to complete our consideration of other possible risk areas, in particular GMP’s arrangements to respond to the review of ‘Operation Augusta’ and the HMICFRS review of the implementation of iOPS. When we have completed our VFM planning considerations we will report any additional significant risks to the Joint Audit Panel.

<table>
<thead>
<tr>
<th>Description of significant risk</th>
<th>Planned response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Financial sustainability</td>
<td>We will review the arrangements GMP has in place for ensuring financial resilience, specifically that the medium term financial plan has taken into consideration factors such as funding reductions, salary and general inflation, demand pressures, restructuring costs and sensitivity analysis given the degree of variability in the above factors. We will also review the arrangements in place to monitor progress delivering the budget and related savings plans.</td>
</tr>
</tbody>
</table>

The 2019/20 net budget was set at £589m, balanced the Home Office Police Grant, GM Precept and the previous years’ Council Tax surplus. Although the police grant for 2019/20 increased by £8.5m and GMP received a £6.6m one-off grant, these increases were predominantly absorbed by the increase of £14.1m relating to unfunded Pension Schemes.

GMP continues to face significant financial challenges but these are not new and are not unique to GMP. However, the challenges do present a significant audit risk in respect of considering the arrangements that GMP has in place to deliver financially sustainability over the medium term.
6. FEES FOR AUDIT AND OTHER SERVICES

Fees for work as GMP's appointed auditor
At this stage of the audit we are not planning any divergence from the scale fees set by PSAA as communicated in our fee letter of 30th April 2019.

<table>
<thead>
<tr>
<th>Service</th>
<th>2018/19 fee</th>
<th>2019/20 fee</th>
</tr>
</thead>
<tbody>
<tr>
<td>External audit of financial statements and value for money conclusion</td>
<td>42,000</td>
<td>42,000</td>
</tr>
</tbody>
</table>

Fees for non-audit work
At this stage, we are not planning to carry out any non-audit work. Before agreeing to undertake any additional work, we will consider whether there are any actual, potential or perceived threats to our independence. Further information about our responsibilities in relation to independence is provided in section 7.
7. OUR COMMITMENT TO INDEPENDENCE

We are committed to independence and are required by the Financial Reporting Council to confirm to you at least annually, in writing, that we comply with the Financial Reporting Council’s Ethical Standard. In addition, we communicate any matters or relationship which we believe may have a bearing on our independence or the objectivity of the audit team.

Based on the information provided by you and our own internal procedures to safeguard our independence as auditors, we confirm that in our professional judgement there are no relationships between us and any of our related or subsidiary entities, and you and your related entities creating any unacceptable threats to our independence within the regulatory or professional requirements governing us as your auditors.

We have policies and procedures in place which are designed to ensure that we carry out our work with integrity, objectivity and independence. These policies include:

- all partners and staff are required to complete an annual independence declaration;
- all new partners and staff are required to complete an independence confirmation and also complete computer-based ethics training;
- rotation policies covering audit engagement partners and other key members of the audit team;
- use by managers and partners of our client and engagement acceptance system which requires all non-audit services to be approved in advance by the audit engagement partner.

We confirm, as at the date of this document, that the engagement team and others in the firm as appropriate, and Mazars LLP are independent and comply with relevant ethical requirements. However, if at any time you have concerns or questions about our integrity, objectivity or independence please discuss these with Mark Dalton in the first instance.

Prior to the provision of any non-audit services Mark Dalton will undertake appropriate procedures to consider and fully assess the impact that providing the service may have on our auditor independence. Included in this assessment is consideration of Auditor Guidance Note 01 as issued by the NAO, and the PSAA Terms of Appointment.

No threats to our independence have been identified.

Any emerging independence threats and associated identified safeguards will be communicated in our Audit Completion Report.
8. MATERIALITY AND MISSTATEMENTS

Summary of initial materiality thresholds

<table>
<thead>
<tr>
<th>Threshold</th>
<th>Initial threshold (£'000s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall materiality</td>
<td>15,000</td>
</tr>
<tr>
<td>Performance materiality</td>
<td>11,250</td>
</tr>
<tr>
<td>Trivial threshold for errors to be reported to the Joint Audit Panel</td>
<td>450</td>
</tr>
</tbody>
</table>

Materiality

Materiality is an expression of the relative significance or importance of a particular matter in the context of financial statements as a whole. Misstatements in financial statements are considered to be material if they, individually or in aggregate, could reasonably be expected to influence the economic decisions of users taken on the basis of the financial statements.

Judgements on materiality are made in light of surrounding circumstances and are affected by the size and nature of a misstatement, or a combination of both. Judgements about materiality are based on consideration of the common financial information needs of users as a group and not on specific individual users.

The assessment of what is material is a matter of professional judgement and is affected by our perception of the financial information needs of the users of the financial statements. In making our assessment we assume that users:

- have a reasonable knowledge of business, economic activities and accounts;
- have a willingness to study the information in the financial statements with reasonable diligence;
- understand that financial statements are prepared, presented and audited to levels of materiality;
- recognise the uncertainties inherent in the measurement of amounts based on the use of estimates, judgement and the consideration of future events; and
- will make reasonable economic decisions on the basis of the information in the financial statements.

We consider materiality whilst planning and performing our audit based on quantitative and qualitative factors.

Whilst planning, we make judgements about the size of misstatements which we consider to be material and which provides a basis for determining the nature, timing and extent of risk assessment procedures, identifying and assessing the risk of material misstatement and determining the nature, timing and extent of further audit procedures.

The materiality determined at the planning stage does not necessarily establish an amount below which uncorrected misstatements, either individually or in aggregate, will be considered as immaterial.

We revise materiality for the financial statements as our audit progresses should we become aware of information that would have caused us to determine a different amount had we been aware of that information at the planning stage.

Our provisional materiality is set based on a benchmark of the 2018/19 gross expenditure at the surplus/deficit on provision of services level. We will identify a figure for materiality but identify separate levels for procedures designed to detect individual errors, and also a level above which all identified errors will be reported to the Joint Audit Panel.

We consider that the gross expenditure at the surplus/deficit on provision of services level remains the key focus of users of the financial statements and, as such, we base our materiality levels around this benchmark.
8. MATERIALITY AND MISSTATEMENTS (CONTINUED)

We expect to set a materiality threshold at around 1.9% of the gross expenditure at the surplus/deficit on provision of services level.

Based on the 2018/19 gross expenditure at the surplus/deficit on provision of services level we anticipate the overall materiality for the year ending 31st March 2020 to be in the region of £15m (£10.653m in the prior year).

After setting initial materiality, we continue to monitor materiality throughout the audit to ensure that it is set at an appropriate level.

Performance Materiality

Performance materiality is the amount or amounts set by the auditor at less than materiality for the financial statements as a whole to reduce, to an appropriately low level, the probability that the aggregate of uncorrected and undetected misstatements exceeds materiality for the financial statements as a whole. Our initial assessment of performance materiality is based on low inherent risk, meaning that we have applied 75% of overall materiality as performance materiality.

We have also calculated materiality for specific classes of transactions, balances or disclosures where we determine that misstatements of a lesser amount than materiality for the financial statements as a whole, could reasonably be expected to influence the decisions of users taken on the basis of the financial statements. We have set specific materiality for the following items of account:

<table>
<thead>
<tr>
<th>Item of account</th>
<th>Specific materiality (£’s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Officer Remuneration bandings</td>
<td>£5,000*</td>
</tr>
<tr>
<td>Related party transactions</td>
<td>£50,000</td>
</tr>
</tbody>
</table>

*Reflecting movement from one salary band to another

After setting initial materiality, we continue to monitor materiality throughout the audit to ensure that it is set at an appropriate level.

Misstatements

We aggregate misstatements identified during the audit that are other than clearly trivial. We set a level of triviality for individual errors identified (a reporting threshold) for reporting to the Joint Audit Panel that is consistent with the level of triviality that we consider would not need to be accumulated because we expect that the accumulation of such amounts would not have a material effect on the financial statements. Based on our preliminary assessment of overall materiality, our proposed triviality threshold is £450k based on 3% of overall materiality.

Reporting to the Joint Audit Panel

To comply with International Standards on Auditing (UK), the following three types of audit differences will be presented to the Joint Audit Panel:

• summary of adjusted audit differences;
• summary of unadjusted audit differences; and
• summary of disclosure differences (adjusted and unadjusted).
ISA (UK) 260 ‘Communication with Those Charged with Governance’, ISA (UK) 265 ‘Communicating Deficiencies In Internal Control To Those Charged With Governance And Management’ and other ISAs (UK) specifically require us to communicate the following:

<table>
<thead>
<tr>
<th>Required communication</th>
<th>Audit Strategy Memorandum</th>
<th>Audit Completion Report</th>
</tr>
</thead>
<tbody>
<tr>
<td>Our responsibilities in relation to the audit of the financial statements and our wider responsibilities</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Planned scope and timing of the audit</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Significant audit risks and areas of management judgement</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Our commitment to independence</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Responsibilities for preventing and detecting errors</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Materiality and misstatements</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Fees for audit and other services</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Significant deficiencies in internal control</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Significant findings from the audit</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Significant matters discussed with management</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Our conclusions on the significant audit risks and areas of management judgement</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Summary of misstatements</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Management representation letter</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Our proposed draft audit report</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
APPENDIX B – FORTHCOMING ACCOUNTING AND OTHER ISSUES

Financial reporting changes relevant to 2019/20

There are no significant changes in the Code of Practice on Local Authority Accounting for the 2019/20 financial year.

Financial reporting changes in future years

<table>
<thead>
<tr>
<th>Accounting standard</th>
<th>Year of application</th>
<th>Commentary</th>
</tr>
</thead>
<tbody>
<tr>
<td>IFRS 16 – Leases</td>
<td>2020/21</td>
<td>The CIPFA/LASAAC Code Board has determined that the Code of Practice on Local Authority Accounting will adopt the principles of IFRS 16 Leases, for the first time from 2020/21. IFRS 16 will replace the existing leasing standard, IAS 17, and will introduce significant changes to the way bodies account for leases, which will have substantial implications for the majority of public sector bodies. The most significant changes will be in respect of lessee accounting (i.e. where a body leases property or equipment from another entity). The existing distinction between operating and finance leases will be removed and instead, the new standard will require a right of use asset and an associated lease liability to be recognised on the lessee’s Balance Sheet. In order to meet the requirements of IFRS 16, all local authorities will need to undertake a significant project that is likely to be time-consuming and potentially complex. There will also be consequential impacts upon capital financing arrangements at many authorities which will need to be identified and addressed at an early stage of the project.</td>
</tr>
</tbody>
</table>
This page is intentionally left blank
PART B

EXCLUSION OF PRESS AND PUBLIC

That, under section 100 (A)(4) of the Local Government Act 1972 the press and public should be excluded from the meeting for the following items on business on the grounds that this involves the likely disclosure of exempt information, as set out in paragraph 3, Part 1, Schedule 12A of the Local Government Act 1972 and that the public interest in maintaining the exemption outweighs the public interest in disclosing the information.