For Information / Consideration	
Public/Non Public*	**Public**
Report to:	**Joint Audit and Scrutiny Panel**
Date of Meeting:	**7th November 2018**
Report of:	**Chief Finance Officer**
Report Author:	**Charlotte Radford**
Other Contacts:	**Brian Welch**
Agenda Item:	**7**

INTERNAL AUDIT PROGRESS REPORT

1. Purpose of the Report

1.1 To provide members with an update on progress against the Internal Audit Annual Plan for 2019-19 and the findings from audits completed to date.

2. Recommendations

2.1 Members are recommended to consider the report and where appropriate make comment or request further work in relation to specific audits to ensure they have adequate assurance from the work undertaken.

3. Reasons for Recommendations

3.1 This complies with good governance and in ensuring assurance can be obtained from the work carried out.

4. Summary of Key Points

4.1 The attached report details the work undertaken to date and summarises the findings from individual audits completed since the last progress report to the panel.

5. Financial Implications and Budget Provision

5.1 None as a direct result of this report.

6. Human Resources Implications

6.1 None as a direct result of this report.

7. Equality Implications

7.1 None as a direct result of this report.

8. Risk Management

8.1 None as a direct result of this report. Recommendations will be actioned to address the risks identified within the individual reports and recommendations implementation will be monitored and reported within the audit and inspection report to this panel.

9. Policy Implications and links to the Police and Crime Plan Priorities

9.1 This report complies with good governance and financial regulations.

10. Changes in Legislation or other Legal Considerations

10.1 None

11. Details of outcome of consultation

11.1 Not applicable

12. Appendices

12.1 Appendix A – Internal Audit Progress Report 2018-19

12.2 Follow up of Audit Recommendations – July 2018

Office of the Police & Crime Commissioner for Nottinghamshire and Nottinghamshire Police

Internal Audit Progress Report 2018/19

October 2018

Presented to the Joint Audit & Scrutiny Panel meeting of: 7th November 2018

Contents

01 Introduction

1.1 The purpose of this report is to update the Joint Audit & Scrutiny Panel (JASP) as to the progress in respect of the Operational Plan for the year ended 31st March 2019 which was considered and approved by the JASP at its meeting on 30th May 2018.

1.2 The Police and Crime Commissioner and Chief Constable are responsible for ensuring that the organisations have proper internal control and management systems in place. In order to do this, they must obtain assurance on the effectiveness of those systems throughout the year, and are required to make a statement on the effectiveness of internal control within their annual report and financial statements.

1.3 Internal audit provides the Police and Crime Commissioner and Chief Constable with an independent and objective opinion on governance, risk management and internal control and their effectiveness in achieving the organisation's agreed objectives. Internal audit also has an independent and objective advisory role to help line managers improve governance, risk management and internal control. The work of internal audit, culminating in our annual opinion, forms a part of the OPCC and Force's overall assurance framework and assists in preparing an informed statement on internal control.

1.4 Responsibility for a sound system of internal control rests with the Police and Crime Commissioner and Chief Constable and work performed by internal audit should not be relied upon to identify all weaknesses which exist or all improvements which may be made. Effective implementation of our recommendations makes an important contribution to the maintenance of reliable systems of internal control and governance.

1.5 Internal audit should not be relied upon to identify fraud or irregularity, although our procedures are designed so that any material irregularity has a reasonable probability of discovery. Even sound systems of internal control will not necessarily be an effective safeguard against collusive fraud.

1.6 Our work is delivered is accordance with the Public Sector Internal Audit Standards (PSIAS).

02 Summary of internal audit work to date

2.1 Since the last progress report to the JASP we have issued three final reports, these being in respect of Force Management of MFSS Arrangements, Corporate Governance and a Follow-up of the Duty Management System audit, the latter being part of the 2017/18 audit plan. We have also issued a report in respect of the Follow-up of Limited Assurance Recommendations (which is reported separately). Additionally, we have issued draft reports in respect of Health & Safety and Commissioning where we await management's responses. Further details are provided in Appendix 1.

Nottinghamshire 2018/19 Audits	Report Status	Assurance Opinion	Priority 1 (Fundamental)	Priority 2 (Significant)	Priority 3 (Housekeeping)	Total
Force Management of MFSS Arrangements	Final	Limited	2	2		4
Code of Governance	Final	Satisfactory		4		4
Health & Safety	Draft					
Commissioning	Draft					
Follow-up of Limited Assurance Recommendations	Final	N/A				
		Total	**2**	**6**	**0**	**8**

2.2 With regards ongoing audits, the audit of Firearms Licensing is in progress. The audits of the Core Financial Systems, IT Strategy and GDPR are scheduled between now and Christmas. Further details are provided in Appendix 2.

2.3 Work in respect of the 2018/19 Collaboration Internal Audit Plan is progressing. We have recently issued the draft report in respect of Strategic Financial Planning, whilst fieldwork in respect of Risk Management has been completed and the draft report will be issued shortly.

03 Performance

3.1 The following table details the Internal Audit Service performance for the year to date measured against the key performance indicators that were set out within Audit Charter.

No	Indicator	Criteria	Performance
1	Annual report provided to the JASP	As agreed with the Client Officer	N/A
2	Annual Operational and Strategic Plans to the JASP	As agreed with the Client Officer	Achieved
3	Progress report to the JASP	7 working days prior to meeting.	Achieved
4	Issue of draft report	Within 10 working days of completion of final exit meeting.	100% (5/5)
5	Issue of final report	Within 5 working days of agreement of responses.	100% (3/3)
6	Follow-up of priority one recommendations	90% within four months. 100% within six months.	Achieved
7	Follow-up of other recommendations	100% within 12 months of date of final report.	N/A
8	Audit Brief to auditee	At least 10 working days prior to commencement of fieldwork.	100% (10/10)
9	Customer satisfaction (measured by survey)	85% average satisfactory or above	None received

Appendix A1 – Summary of Reports

Below we provide brief outlines of the work carried out, a summary of our key findings raised and the assurance opinions given in respect of the final reports issued since the last progress report:

Implementation of Duty Management System – Follow-up

Assurance Opinion – 2016/17	**Limited**
Assurance Opinion – 2017/18	**Satisfactory**

Recommendation Priorities		
	2016/17	**2017/18**
Priority 1 (Fundamental)	3	1
Priority 2 (Significant)	3	2
Priority 3 (Housekeeping)	0	1

As part of the Internal Audit Plan for 2017/18 for the Office of the Police and Crime Commissioner for Nottinghamshire (OPCC), and Nottinghamshire Police we undertook a follow-up audit of the controls and processes in place for the Implementation of the Duty Management System (DMS).

An audit of the Implementation of DMS was undertaken during 2016/17 which resulted in a limited assurance opinion with regards the adequacy and efficiency of controls that were in place. Therefore, to ensure that the control weaknesses previously highlighted have been addressed, a follow-up audit has taken place. The specific areas that formed part of the original review included: policies, procedures, guidance, training, system access, user controls and data reconciliation.

During the last audit visit there were weaknesses in the system of internal controls that put the Organisation's objectives at risk and whilst the system itself had the capabilities and controls for restricting access to personal data, the governance arrangements which underpin the implementation of DMS needed clarification. Whilst improvements have been made, and the previous recommendations have been partly implemented, there are still improvements to be made.

The Follow-up audit confirmed that progress had been made to address the previously identified weaknesses, although there remained some work to do.

We raised one priority 1 recommendation of a fundamental nature that required addressing. This is set out below:

Recommendation 1	The Force should clarify the roles and responsibilities of the parties involved in the maintenance and usage of the DMS System. The Force should confirm where the responsibility for system administration will lie. Once the responsibilities are clear, the Force should ensure that the System Administrators reports are being used to maintain the system. The Information Asset Register should be updated to ensure the information asset owners and their delegates are correctly stated.

Finding	**System Governance – System Maintenance** During the last audit visit there was a lack of ownership over the Duty Management System, including responsibility for the information, security of information and maintenance of the information within the system. Some improvements have been made and an Information Asset Owner has been assigned for the data that is held within DMS. It was, however, noted that one of the delegates listed on the Information Asset Register was out of date and required updating. However, discussion with HR confirmed that system administration responsibility is currently under discussion as to where this will sit moving forward following the previous DMS Lead within RMU leaving the organisation. The lack of ownership for system administration was highlighted during the audit when confirmation that APEX reports are now available for system administrators, however these are currently not being regularly used.
Response	a) OSD is responsible for the DMS system. b) Superintendent Operational Support is the Information Asset Owner. c) Sergeant within Duties Management will manage the System Administrators. The number of administrators has been reduced and administration will be shared with Duty Planners. Action – Duty Management Sergeant to ensure reports are being used to maintain the system. d) Information Asset Register will be updated to reflect correct delegates. Action – Superintendent Operational Support to update Information Asset Register as appropriate.
Timescale	a) Complete b) Complete c) October 2018 d) August 2018

We also raised two priority 2 recommendations where we believe there is scope for improvement within the control environment. These are set out below:

- An alternative solution to the automated reconciliation between the data in DMS and the data in Oracle should be put in place to provide assurance that the data held within DMS reconciles to the Oracle system.

  Both HR and the RMU should work together to review the reporting capabilities of both systems and work out the most effective way to carry out the manual reconciliations on a regular basis.

- To ensure data in Oracle and DMS is clearly reconciled, the back log of rejections should be cleared in a timely manner. Moreover, when reviewing the data rejection log the list should be all historic errors rather than focus on current week to prevent historic errors being missed.

  Consideration should be given to maintaining a log of the rejections that occur so that an analysis of common issues can be compiled. This would enable the root causes to be identified and addressed, reducing the need for continuous manual processing.

Management indicated that both recommendations will be implemented by the end of October 2018.

Force Management of MFSS Arrangements

Assurance Opinion	Limited

Recommendation Priorities	
Priority 1 (Fundamental)	2
Priority 2 (Significant)	2
Priority 3 (Housekeeping)	-

Contracts

Contractual arrangements clearly set out roles and responsibilities of the relevant parties. The contract contains clear and measurable requirements against which contractor performance can be monitored.

Variations

Additions, changes and deletions to the service are clearly set out in the contract and include defined approval arrangements.

Service Level

There are clear service levels which sets out the requirements and standards the Force expects from the contract.

Ad hoc Works

There are robust arrangements in place for the communication and approval of additional services.

Quality Control, Rectification and Default

Sub-standard, incorrect, incomplete and non-delivered services are identified and subsequent management corrective action taken.

There are clear arrangements in place for the deduction of penalties or non-payment of incentivised bonuses in the event of sub-standard, incorrect, incomplete and non-delivered services.

Payments

Payments made to the contractor are in accordance with the contract. Performance Monitoring

There is a robust process of performance monitoring in place that ensures that the quality of services is in accordance with Force requirements.

Budgetary Control

Budgets are effectively monitored and under/overspends are promptly identified and addressed.

We raised two priority 1 recommendations of a fundamental nature that require addressing. These are set out below:

Recommendation 1	The Force should raise the lack of budget setting procedures with the appropriate governance forum to ensure an effective budget setting process can be embedded and is aligned with their own budget setting process. The Force should ensure that the Chief Finance Officers are clearly included in any budget setting process and should be members of the appropriate governance forum where this is scrutinised as part of the budget setting process. The Force should ensure the late delivery of budget monitoring information from MFSS is escalated as soon as possible and actions taken to address are put in place.
Finding	**Financial Planning** The terms of reference for the Joint Oversight Committee (JOC) states it is their responsibility *to determine the annual budgets and MTFP's*" of MFSS. The current members of this Committee are the Police and Crime Commissioners and the Chief Constables of the partners, however, it was noted that the Chief Finance Officers are not listed as members of this committee. Upon review Audit confirmed that there is currently no agreed process or timetable for setting the MFSS budget on an annual basis. A review of the 2017/18 budget approval found that whilst it was approved at the Joint Oversight Committee, it was not further scrutinised at the Management Board prior to approval, as had been requested by the JOC, due to a timing issue. The 2018/19 budget for MFSS has still to be approved. A contributory factor being the failure to on-board new partners as anticipated and the impact this will have on the costs borne by the existing partners. The lack of agreed budget poses a significant risk for the Force. On a quarterly basis MFSS provide the Force with a breakdown of the costs it has incurred, alongside a budget monitoring spreadsheet detailing the actual costs versus the budgeted costs and then invoices the Force for its agreed proportion of these costs alongside the other partners. Audit were informed that often this information can be late from MFSS, but it was not escalated accordingly.
Response	a) The lack of budget setting procedures has been raised on numerous occasions by the CFO-PCC and the force Project Managers – Grant Thornton. b) There is no CFO representation on the Joint Oversight Committee. This committee is responsible for budget setting. This issue has been raised by Joint CFO's-PCC and Joint CFO's – CC. A response is currently awaited from the Joint Oversight Committee. c) Agreed, Arrangements have already been agreed with the new CEO of MFSS to brief CC/CFO's on production of MFSS budgets at an early stage.
Timescale	a) Complete. b) On-going. c) On-going – will be reviewed as part of the 19/20 budget build.

Recommendation 2	The current lack of formally approved SLA's and KPI's should be escalated to the relevant governance forum and a timetable put in place for the delivery and approval of effective performance indicators. The Force should review the performance information that would be most relevant at each of the governance forums, then work with MFSS to ensure they receive this information. The number of individual complaints raised and managed by MFSS should be centrally co-ordinated by the Force and form part of the service review meeting to ensure effective performance management.
Finding	**Performance Management** It has been acknowledged by the Force that there are no agreed service level agreements or key performance indicators between the Force and MFSS. Audit were informed work is on-going to finalise these and put them in place. In the meantime it was noted that some interim KPI's are being presented at the Service Review Meeting between the Force and MFSS. These are currently focused on Finance and HR specifically and no overall review of total services is able to be effectively carried out. Audit found that the performance information that was provided to the Joint Oversight Committee was the same as the performance information provided at the Management Board. These groups have a different focus (strategic versus operational) and therefore would require differing information to allow for effective oversight and scrutiny of MFSS performance across the totality of services provided. From the performance information that was provided to the Force, there was a lack of analytical information that would allow context and root causes to be identified. One omission from the performance data was the number of errors that had occurred throughout the different services provided. MFSS have a complaints process that should be followed when individuals are not happy with the level of service received. They will investigate and resolve the matter within a set time frame. However, it was noted that the number of complaints received, investigated and resolved are currently not reviewed or reported to any of the governance forums.
Response	a) Service Level Agreements, including KPI's are under review with no agreement at present. b) The Service Improvement Group (SIG) currently reviews management information presented at the Management Boards and Joint Oversight Committees. The force is represented at all 3 meetings. c) A new role has been put in place to manage complaints; co-ordinating across the force. KPI's are currently being developed, and service reviews are held on a monthly basis, where customer complaints are discussed and opportunities to influence process are identified and fed back.
Timescale	a) March 2019 b) On-going c) On-going

We also raised two priority 2 recommendations where we believe there is scope for improvement within the control environment. These are set out below:

- The Improvement Plan should be updated to include target completion dates for activities to ensure MFSS and Partners are held to account for non-delivery of activities, the Force should raise this at the Optimisation Board.

- The Force should put in place appropriate co-ordination and communication internally between the Forces' attendees at the MFSS governance forums to ensure the key information is shared.

  The Force should seek clarity from MFSS and partners to confirm the roles of each governance forum, as well as ensuring the BPT's are operating as intended.

  The role of the HR Business Partner should be clearly defined and communicated across the Force.

Corporate Governance

Assurance Opinion	Satisfactory

Recommendation Priorities	
Priority 1 (Fundamental)	-
Priority 2 (Significant)	4
Priority 3 (Housekeeping)	-

Our audit considered the following risks relating to the area under review:

- The roles and responsibilities of senior officers and staff within the Force and OPCC are clearly defined, particularly regarding their decision making responsibilities.
- The corporate governance framework is supported by policies and procedures, such as a decision making framework and scheme of delegation and that these are appropriately communicated.
- Each governance forum across the Force and OPCC has an appropriate terms of reference that clearly defines their decision making responsibilities.
- Decisions made are clearly recorded, communicated and published where relevant.
- Decisions are made in accordance with the governance framework in a clear and transparent manner, supported by the appropriate levels of relevant and timely information.
- The OPCC has appropriate oversight of decisions made at the Force through regular reporting or escalation of decisions made.

We raised four priority 2 recommendations where we believe there is scope for improvement within the control environment. These related to the following:

- The Corporate Governance Framework should be reviewed and formally approved. Once approved, it should be communicated to staff and made available via the intranet and external website.

  Once the review has been finalised, the Corporate Governance Framework should be reviewed regularly to ensure it remains reflective of current working practices. Responsibility for the review should be assigned to a Senior Officer to ensure the review is carried out.

- A Policy Review Log should be developed detailing the scheduled review dates for policies and procedures, as well as the officer who approved the policy.

  Responsibility should be assigned for monitoring the Policy Review Log to help ensure compliance.

- The Force should share decision/action logs with the OPCC to ensure transparency where the OPCC are unable to attend meetings.

- A call in procedure should be developed for urgent decisions made outside of the relevant committee meetings.

  Each urgent decision form should be circulated amongst the COT, members of the relevant governance committee and a representative from the OPCC to allow the opportunity for the decision to be called into the next meeting for further scrutiny and challenge.

Management confirmed that where action was not taken immediately, the recommendations would be implemented by the end of March 2019.

Appendix A2 Internal Audit Plan 2018/19

Auditable Area	Planned Fieldwork Date	Draft Report Date	Final Report Date	Target JASP	Comments
Core Assurance					
Core Financial Systems	Nov 2018			Mar 2019	ToR agreed; starts 26th Nov.
Code of Governance	Sept 2018	Aug 2018	Oct 2018	Nov 2018	Final report issued.
Strategic & Operational Risk					
Partnership Working	Mar 2019			June 2019	
Commissioning	Sept 2018	Oct 2018		Nov 2018	Draft report issued.
Force Management of MFSS Arrangements	June 2018	June 2018	July 2018	Nov 2018	Final report issued.
IT Strategy	Nov 2018			Mar 2019	Deferred from Q1 to allow IT Strategy to be finalised.
Seized Property	Mar 2019			June 2019	Deferred from Oct 2018 on management's request.
GDPR	Nov 2018			Mar 2019	
Health & Safety	Sept 2018	Oct 2018		Nov 2018	Draft report issued.
Firearms Licensing	Oct 2019			Mar 2019	Brought forward from March 2019; work in progress.
Follow-up of Limited Assurance Recommendations	July 2018	July 2018	July 2018	Nov 2018	Final report issued.

Auditable Area	Planned Fieldwork Date	Draft Report Date	Final Report Date	Target JASP	Comments
Collaboration					
Risk Management	Aug 2018			Nov 2018	Fieldwork completed; being reviewed.
Strategic Financial Planning	July 2018	Oct 2018		Nov 2018	Draft report issued.
Business Planning	Sept 2018			Nov 2018	Work in progress.
Review of Collaboration Assurance Statements	May 2018	May 2018	June 2018	July 2018	Final memo issued.

Appendix A3 – Definition of Assurances and Priorities

Definitions of Assurance Levels		
Assurance Level	**Adequacy of system design**	**Effectiveness of operating controls**
Significant Assurance:	There is a sound system of internal control designed to achieve the Organisation's objectives.	The control processes tested are being consistently applied.
Satisfactory Assurance:	While there is a basically sound system of internal control, there are weaknesses, which put some of the Organisation's objectives at risk.	There is evidence that the level of non-compliance with some of the control processes may put some of the Organisation's objectives at risk.
Limited Assurance:	Weaknesses in the system of internal controls are such as to put the Organisation's objectives at risk.	The level of non-compliance puts the Organisation's objectives at risk.
No Assurance	Control processes are generally weak leaving the processes/systems open to significant error or abuse.	Significant non-compliance with basic control processes leaves the processes/systems open to error or abuse.

Definitions of Recommendations	
Priority	**Description**
Priority 1 (Fundamental)	Recommendations represent fundamental control weaknesses, which expose the organisation to a high degree of unnecessary risk.
Priority 2 (Significant)	Recommendations represent significant control weaknesses which expose the organisation to a moderate degree of unnecessary risk.
Priority 3 (Housekeeping)	Recommendations show areas where we have highlighted opportunities to implement a good or better practice, to improve efficiency or further reduce exposure to risk.

Appendix A4 - Contact Details

Contact Details

David Hoose	07552 007708 David.Hoose@Mazars.co.uk
Brian Welch	07780 970200 Brian.Welch@Mazars.co.uk

A5 Statement of Responsibility

Status of our reports

The responsibility for maintaining internal control rests with management, with internal audit providing a service to management to enable them to achieve this objective. Specifically, we assess the adequacy of the internal control arrangements implemented by management and perform testing on those controls to ensure that they are operating for the period under review. We plan our work in order to ensure that we have a reasonable expectation of detecting significant control weaknesses. However, our procedures alone are not a guarantee that fraud, where existing, will be discovered.

The contents of this report are confidential and not for distribution to anyone other than the Office of the Police and Crime Commissioner for Nottinghamshire and Nottinghamshire Police. Disclosure to third parties cannot be made without the prior written consent of Mazars LLP.

Mazars LLP is the UK firm of Mazars, an international advisory and accountancy group. Mazars LLP is registered by the Institute of Chartered Accountants in England and Wales to carry out company audit work.

/

OPCC for Nottinghamshire & Nottinghamshire Police

Follow up of Audit Recommendations – July 2018

01 – Introduction

As part of the Internal Audit Plan for 2018/19 for the Office of the Police and Crime Commissioner for Nottinghamshire (OPCC) and Nottinghamshire Police we have undertaken a follow-up review of Internal Audit recommendations made. This report provides an overview of activity undertaken to verify the implementation of audit recommendations made as a result of 2016/17 and 2017/18 audits that provided a 'limited' assurance opinion. The audits covered in this review were Road Safety Partnership, Risk Management and Data Protection Act. The review focused on all the recommendations made (see Appendix 1) where agreed implementation dates had now passed.

This report covers only those limited assurance audit reports where a dedicated follow-up has not been completed or planned. The following provides the status of the limited audit reports issued in 2016/17 and 2017/18 reports where recommendation dates have been reached:

Audit / Recommendation	Priority	Recommendations			Audit Confirmed Implemented	Comments
		Agreed Implementation Date	Manager Confirmed Implementation	Manager Confirmed Not Implemented		
Road Safety Partnership (February 2018)	Four recommendation raised – two P1 and two P2					
- Strategy	P1	June 2018	N/A	Yes	N/A	Recommendation due to be implemented for year end 18/19.
- Budget Deficit	P1	March 2018	Yes	N/A	Yes	Recommendation implemented.
- Charging Guidance	P2	March 2018	N/A	Yes	N/A	Partially Implemented
- Annual Report	P2	May 2018	N/A	Yes	N/a	Recommendation due to be implemented for year end 18/19.
Risk Management (March 2017)	Seven recommendations raised – six P2 and one P3					
- OPCC Strategy	P2	August 2017	Yes	N/A	Yes	Recommendation implemented.
- Training	P2	August 2017	N/A	Yes	N/A	Recommendation Pending.
- Removal of Risks	P3	August 2017	Yes	N/A	Yes	Recommendation implemented.
- Alignment of Registers	P2	August 2017	Yes	N/A	Yes	Recommendation implemented.
- Completeness of Registers	P2	August 2017	Yes	N/A	Yes	Recommendation implemented.
- Format of Registers	P2	August 2017	Yes	N/A	Yes	Recommendation implemented.
- Overview of Risk Registers	P2	August 2017	Yes	N/A	Yes	Recommendation implemented.

Audit / Recommendation	Priority	Recommendations			Audit Confirmed Implemented	Comments
		Agreed Implementation Date	Manager Confirmed Implementation	Manager Confirmed Not Implemented		
Data Protection Act (October 2016)	Nine recommendations raised – one P1, five P2 and three P3					
- Policies & Procedures	P2	December 2016	Yes	N/A	Yes	Recommendation Implemented.
- IAO Job Descriptions	P3	March 2017	Yes	N/A	Yes	Recommendation Implemented.
- IAO Training & Handbook	P2	March 2017	N/A	Yes	N/A	Partially Implemented.
- List of IAO's & Delegates	P3	November 2016	Yes	N/A	Yes	Recommendation Implemented.
- Completeness of IA Register	P2	November 2016	N/A	Yes	N/A	Partially Implemented.
- Format of IA Register	P3	November 2016	N/A	Yes	N/A	Partially Implemented.
- Information Risk System	P1	March 2017	Yes	N/A	Yes	Recommendation Implemented.
- Audit Role	P2	December 2016	Yes	N/A	Yes	Recommendation Implemented.
- Audit Process	P2	March 2017	Yes	N/A	Yes	Recommendation Implemented.

02 – Follow-Up Results

Road Safety Partnership (Final Report February 2018)

Summary

As part of the follow up meetings audit were informed that the Nottingham Strategic Road Safety Partnership (NSRSP) is the regional approach to all elements of Road Safety and as part of this it includes a Nottingham Educational Road Safety Partnership (NESP) and Nottingham Camera Safety Partnership (NCSP). The NCSP is the partnership that was reviewed in the February 2018 report, however there were areas of cross over with the NSRSP.

The Camera Safety Partnership Team at the Force from the 1st May 2018 is now under the command of the Operational Support Department which is led by Superintendent Stephen Cartwright who acts as the Strategic Lead for the NCSP. There is a lack of clarity in the relationship between the NSRSP and the NCSP and the strategic lead is currently liaising with the partners in the region so that a clear strategy and plan can be developed to take the NCSP forward effectively.

A key weakness noted in the audit report was the previous budget deficits that had caused a low level of reserves, however this has been rectified and audit confirmed reserves for the NCSP have been replaced and have been increased beyond the original position. A review of the NCSP has been undertaken and a briefing report has been drafted, which will be used to drive forward further improvements at the unit however, at the time of the audit follow up visit, these improvements were work in progress. A full breakdown of each recommendation and audit findings are noted below.

Finding	Recommendation	Initial Management Comments	Follow Up Result	Result / Timeframe of Risk Exposure
RSP Strategy *Observation*: The RSP Strategy defines the objectives of the partnership. Audit noted that the strategy had last been reviewed on 9th May 2008. The strategy was reviewed by audit which confirmed that it did not clearly define roles and responsibilities of partners in regards to managing the RSP's finances and how joint funding of activities would be achieved. A date of next review was not included. *Risk:* Where the RSP strategy does not reflect the financial responsibilities of the partners, there is an increased risk that the RSP lacks a joined up approach to co-ordinating resources to fund activities.	**Priority 1:** The RSP Strategy should be reviewed and updated to ensure that it is aligned with the aims and objectives of its partners. The Strategy should explicitly set out the roles and responsibilities of partners and, in particular, the management of the RSP's finances and each partners responsibilities for joint funded activities.	There is a review underway within the force, being led by the DCC. All partners should be involved in formulating the strategy. DCC June 2018	The RSP Strategy referred to in the original finding is the strategy for the Nottingham Strategic Road Safety Partnership, not the Nottingham Camera Safety Partnership. However, the NCSP intends to develop its own strategy that will align to the overall strategy of the region for Road Safety so that there is a clear way of working moving forward.	Not Implemented - due to be implemented by end of 2018/19.

RSP Budget Deficit *Observation:* The RSP had a budget deficit of £370,168.21 for 2016/17. As a result, the RSP drew down on its reserve fund for this same amount, reducing the fund to £1,059,097.37. The RSP no longer receives funding from Nottinghamshire City Council and County Council and must ensure that it is entirely self-funded. The Force presently provides, on an annual basis, £129,000 and £129,689 to the City Council and County Council respectively for road safety educational posts. It was identified through discussions with the Senior Management Accountant that the Force is presently in negotiations with the City Council and County Council to reduce these payments. *Risk:* Where over expenditure occurs, there is an increased risk that the RSP experiences a budget deficit leading to financial instability and a requirement to draw on its reserve fund.	**Priority 1** A corrective action plan should be put in place to determine the income and expenditure of the partnership to ensure that a budget deficit for 2017/18 does not occur.	Agreed Lead Officer RSP March 2018	A review of the reasons for the budget deficit was undertaken and this highlighted timing issues with the invoices received from the councils in regards to the money that is paid to them for road safety education posts. This meant they were charged twice during 2016/17 by accident. Therefore, these sums were not paid in 2017/18 and therefore the reserves were able to be replenished. As at the end of 2017/18, total income exceeded expenditure and the deficit that was made up from reserves previously was replaced and, therefore, at the end of 2017/18 the reserves position was at £1,386,055.	Recommendation Implemented.
Charging Guidance *Observation:* As referred to in 4.3 above, the RSP had a budget deficit of £370,168.21 for 2016/17, with there being ongoing discussions with the City and County Councils around the financing of the Partnership. Given the current financial pressures on the RSP, and its Partners, it is important that clear guidance is available to both Finance and officers in respect of what can and cannot be charged to the partnership budget. *Risk:* The partnership budget remains in deficit, partly due to inappropriate items of expenditure being charged to it.	**Priority 2** Clear guidance should be produced, and communicated to the relevant staff / officers, with regards what is deemed to be relevant expenditure and can be charged to the partnership budget.	Agreed DCC May 2018	The new strategic lead for the partnership at the Force has reviewed the approach that the NCSP will take moving forward. The unit will adopt the Treasuries 'Managing Public Money' guidance and the National Driver Offender Rehabilitation Scheme (NDORS), where it receives income from. This will provide clarity on the income and expenditure that will be charged to the partnership budget. Audit were informed that this commitment will form part of the new NCSP Strategy.	Partially Implemented. To be formally agreed at the quarterly joint steering group and to be included in the Strategy.
RSP Annual Report *Observation:* The RSP Strategy sets out its aims and objectives as being: • Reduce casualties on Nottinghamshire's roads and better the national casualty reduction targets by 2020.	**Priority 2** The RSP should be required to produce an annual report which, amongst other things, sets out actual performance against it	Agreed DCC May 2018	The partnership has been in a state of flux due to the change in the Operational Support department at the Force and, as such, an annual report for 2017/18 was not able to be completed.	Not Implemented. Due to be completed for 2018/19.

• Bring together those organisations with a remit to reduce road casualties to encourage and facilitate better co-ordination of their activities. • Maximise the effectiveness of resources and activities being directed at casualty reduction. However, audit found no evidence that an annual report was produced which was presented to the relevant forum to demonstrate the performance of the Partnership, including its financing from each of the partners. *Risk:* Where performance and financial inputs are not reported, there is a risk that timely remedial action is not provided and / or the financial arrangements for the Partnership are not transparent.	strategic aims, and provides a transparent record of expenditure made against the partnership budget.		However, the new strategic lead has tasked the partnership to deliver a clear annual report for 2018/19. This will include the finances of the partnership and the relevant performance data that the partnership has delivered.	

Risk Management (Final Report March 2018)

Summary

The management of risk and business continuity currently sits within the Corporate Services department at the Force and the Deputy Chief Constable is the Chief Officer lead for Risk Management. As part of the follow up meetings audit were informed that there is a review of the current structure within the Force and therefore the responsibility for managing risk may be moved, As a consequence, one of the recommendations were on hold pending the outcome of the review.

The Force acknowledged that the management of risk had slipped due to competing priorities and reduced resources, however they fully accepted the findings of the audit and the new Deputy Chief Constable has acted as the lead to address the issues highlighted and improve the Forces' risk management approach. Audit were informed that there will be ongoing developments to the current approach as the DCC looks to follow South Yorkshire Polices' approach to risk management, an approach that recently won a CIPFA Award for Good Governance. However, whilst this is the future plan for the process, it was clear from the evidence provided to audit that improvements have been made to the existing system and a full breakdown of each recommendation and audit findings is noted below.

Finding	Recommendation	Initial Management Comments	Follow Up Result	Result / Timeframe of Risk Exposure
OPCC Risk Management Strategy *Observation*: The Force have a Corporate Risk Management Strategy that has recently been approved. The Strategy includes: • The strategic direction of the Force's attitude to risk; • The level and nature of risk that is deemed acceptable (risk appetite); • The Force's risk tolerance threshold; and • Risk priorities for the current year. At the time of the audit it had not been agreed that the OPCC would adopt the Force's Risk Management Strategy. *Risk*: Where the OPCC's appetite, tolerance and attitude toward risk is not detailed in a strategy, there is a risk that staff could accept an inappropriate level of risk.	**Priority 2** A Risk Management Strategy should be developed for the OPCC; this should include: • The strategic direction of the OPCC's attitude to risk; • The level and nature of risk that is deemed acceptable (risk appetite); • The OPCC's risk tolerance threshold; and • Risk priorities for the current year.	Risk and Business Continuity Officer to liaise with OPCC in regard to creating an appropriate Joint Corporate Risk Management Strategy. Risk & Business Continuity Officer OPCC 31st August 2017	The Force have worked with the CEO at the OPCC and this has resulted in a joint Risk Management Strategy being approved and put in place in June 2017. The strategy includes both Organisations: *"The purpose of this joint Force and Nottinghamshire Office of the Police and Crime Commissioner (NOPCC) Risk Management Strategy is to outline an overall approach to risk management that addresses the risks facing the Force and NOPCC in achieving their objectives, and which will facilitate the effective recognition and management of such risk".* Audits a review of the Strategy confirms that Strategic Direction, Risk Appetite and a Tolerance Threshold are all included. The OPCC Strategic Risk Register has recently been reviewed against the Commissioner's new Police & Crime Plan. The outcome of this work will be reported to Audit & Scrutiny Panel at the November meeting.	Recommendation Implemented.

Risk Management Training *Observation*: Audit confirmed with the Risk and Business Continuity Officer that training is currently provided to risk register owners on an ad hoc basis, however there are currently no records maintained of who received training or when this was provided. At present there are no training courses or materials in place to assist staff across the Force and OPCC in managing risks. *Risk*: Staff do not have the appropriate level of training to effectively manage risks at the Force and OPCC.	**Priority 2** The Force and OPCC should ensure that staff receive appropriate training on risk management	The Risk and Business Continuity Officer will develop in-house training based on the force's internal policy and procedure. This will be delivered to all Heads of Department and equivalent. A user guide will also be written to support the adoption of the force's policy and procedure, to ensure staff are clear on the escalation and review processes within risk management. Risk & Business Continuity Officer 31st August 2017	Audit were informed that the DCC has committed the funds to enable one of the Risk & Business Continuity Officers to become an accredited Risk Trainer, however due to the review of the department that is ongoing this is on hold pending the outcome of the review. It is envisaged that formal training within both the Force and OPCC will commence once this decision has been made. Informally, audit were informed that the Risk & Business Continuity Officers at the Force have met with each Risk Register owner to ensure they are aware of the correct risk management processes that should be followed.	Recommendation Pending.

Removing Risks from Registers *Observation*: Audit confirmed that there is a combined Risk Management Policy and Risk Management Procedure in place for the Force and the OPCC. The Policy and Procedures are detailed and include key areas such as: • Roles and Responsibilities • Risk Identification • Risk Analysis • Risk Scoring and Review • Risk Monitoring However, internal audit noted that there was no coverage of the process to be followed when a risk was to be removed from a risk register. *Risk*: Identified risks are inappropriately removed from the risk registers in place	**Priority 3** The Risk Management Policy and/or Procedures should be updated to include the process to be followed when a risk is being removed from a risk register. This should include details of who needs to approve the removal and how this should be documented.	The Risk and Business Continuity Office will update the force's procedure to reflect the process of what should happened when a risk is removed from a risk register. Risk & Business Continuity Officer 31st August 2017	The Force have updated the Corporate Risk Management Procedure and, effective from December 2017, a removal of risk process has been included. This states: *'When a Risk has been reviewed and is considered for removal then a full explanation should be documented on the risk register together with the rational by the risk owner. This should contain why they believe the risk no longer exists or controls and actions that mitigate the risk together with why they believe it is no longer appropriate to be on the risk register. Before the risk is removed the risk register must be endorsed by the relevant Departmental Head if a Departmental Risk and DCC if a Strategic one. This provides effective governance and audit trail for future reviews.'* As a consequence, a clear approval and audit trail is now required. Audit confirmed the new approach through review of the current departmental risk registers.	Recommendation Implemented.

Alignment of Risk Registers *Observation*: The governance statement completed by departments state that they escalate high risks to the Force Strategic Risk Register through the Risk and Business Continuity Officer. The CRM Strategy states all risks that are scored as high should be escalated. Audit compared the high risks on five departmental risk registers and found that not all were clearly stated on the strategic risk register. Discussion with the Risk and Business Continuity Officer found that not all high risks on departmental registers will be included on the Strategic Risk Register if the Deputy Chief Constable feels they are being adequately managed within the risk appetite of the Force. However, this decision is not documented at present. *Risk:* The Strategic Risk Register does not represent all risks to the organisation.	**Priority 2** Decisions made by the Deputy Chief Constable not to escalate high risks on departmental risk registers to the strategic risk register should be documented.	The Risk and Business Continuity will review the current risk appetite to ascertain whether all high/very high risks are reviewed at the right level. Consideration will also be given to adopting a residual risk score to assist in seeing whether risks being managed require escalation. At the monthly DCC meetings comments will be added to departmental risk registers outlining discussions on escalation. Risk & Business Continuity Officer 31st August 2017	The Force have updated their risk management procedures to show the new approach. Under the Risk Monitoring section it states: "*Where the DCC considers that it is appropriate that a high risk should be managed at a Departmental level then this decision should be fully documented on the register to provide an audit trail and ensure clarity for governance."* As part of the monthly monitoring undertaken by the DCC, the Risk & BC Officer provides a summary of the high risks from all risk registers to allow this review to take place. A copy of this summary was provided to audit to confirm the process has been embedded.	Recommendation Implemented.

Completeness of Risk Registers *Observation*: Audit testing of a sample of eight strategic and departmental risk registers identified a variety of gaps in the information recorded. • The Risk Register for the Intelligence service area was considered to be incomplete, as risks had not been assigned scores or owners and the additional controls, interdependencies, status, and review date columns had not been populated. Furthermore, risk six on the register did not have any specified existing controls. • There were four cases identified where risks did not have any associated existing mitigating controls or response plans noted. These were risks NPF0024 on the Force Strategic Register; OPCC009 on the OPCC Strategic Register; reference six on the Intelligence Risk Register; and a risk on the Human Resources Risk Register, which had not been given a reference number. • Risks (NPF011 & NPF007) were duplicated on the Force Strategic Risk Register. *Risk*: The Force is exposed to risk above its appetite through failure to record, monitor and control the risks it faces.	**Priority 2** All risk registers for the Force should be recorded in line with the Risk Management Policy / Procedures. Sufficient detail should be recorded for each identified risks, including: • Risk scores; • Mitigating actions; • Risk owners. The Force Strategic Risk Register should be reviewed and one of the risks that are duplicated should be removed (NPF011 & NPF007).	The Risk and Business Continuity Officer will review the Corporate Risk Register for any duplication. All departmental risk registers will also be reviewed to ensure completeness and that key information is included. Risk & Business Continuity Officer 31st August 2017	Audit were provided with a sample of the departmental risk registers and were able to confirm through a review of registers that they were fully completed. Additionally, the risks that were identified as duplicate previously have been reviewed. Both have been retained but have been reworded as they related to two different issues and are included on the Estates Register for ongoing monitoring.	Recommendation Implemented.

Format of Risk Registers *Observation*: Examination of the strategic risk registers and a sample of eight departmental risk registers found that risk registers are not created in a standard format and that some key pieces of information are not currently recorded. In order for the Force and OPCC to be able to effectively and consistently manage its risks across the business, a template should be created so that all registers follow the same format. *Risk*: Inconsistent approach to managing risks across the Force and OPCC.	**Priority 2** A standard format for the registers should be produced This should include the following detail: • A front sheet detailing the business area, risk register owner, and period for which the risk register relates; • The date the risk was added to the register • Risk details; • An assigned owner for each risk; • The inherent risk score for each risk, • Any mitigating actions that are in place, or should be implemented; • The residual risk that remains after mitigating actions have been applied; • The date the risk was last reviewed and the date the next review is due; Any closed risks.	Risk and Business Continuity Officer will ensure a consistent format is adopted across the force. The longer term IT solution will be discussed with the DCC to ascertain whether funds are available for this facility. Risk & Business Continuity Officer 31st August 2017	As per the comments above with regards to completeness of registers, it was confirmed that for the sample of risk registers provided that they are now all in the same format. The only exception to the format, at present, is the OPCC Risk Register, however work is ongoing between the Risk & BC Officers and the OPCC Risk Register Owner, the OPCC CEO, to align these with the Force.	Recommendation Implemented.

Overview of all Risk Registers *Observation*: The Departmental risk registers are reviewed by Senior Management Teams within that department. However, there is currently no central oversight of these registers to confirm that reviews are taking place in a timely manner. Moreover, the departmental risk registers are not saved or available in a central place, as they are saved within departments. Therefore, at any point in time, all risks in relation to the Force are not collated in one place. *Risk*: The Force and OPCC are unaware of all risks that the organisations are facing and that all identified risks are being appropriately managed.	**Priority 2** A process should be in place to confirm that the departmental risk registers are being reviewed in a timely manner. Consideration should be made for central oversight of all risk registers to give assurance of timely update and regular monitoring if risks across the Force.	Risk and Business Continuity Officer will ensure the DCC sample checks department risk registers on a monthly basis. A shared drive will also be created (as an interim solution) and all departmental risk registers will be held there. The longer term IT solution will be discussed with the DCC to ascertain whether funds are available for this facility. Risk & Business Continuity Officer 31st August 2017	The Risk and Business Continuity Officer diaries the monthly reviews of Risk Registers with the DCC so that they are carried out on a rolling basis and all the registers are covered. From a review of the sample of current risk registers, audit can confirm that timely updates have been made against the risks in the register. There has been a commitment to adopting an IT solution for the management of the risks moving forward and the Force has been working with colleagues in the region to seek a value for money approach. However, current changes in circumstances at the other Forces have slowed this progress and the Force is considering the best options to take forward.	Recommendation Implemented.

Data Protection Act (Final Report October 2016)

Summary

Since the last audit visit the Information Management Team has been through a number of changes, which included a reduction in the size of the team following a Force restructure in 2016 and was rolled out during 2017. The team lost the Information Security Officer at the end of 2016, although they were able to recruit into this role in the summer of 2017.

There has been high levels of demand for Subject Access Requests and Freedom of Information requests being handled by the Disclosure Team which led to significant backlogs. In addition, a Records Management function has been established as part of the Information Management Team and over the last twelve months they have been gathering information on the records that are held across the Force which has helped the Force to understand the information it holds and where it is being held.

The Information Management Lead has worked with the Performance Improvement Group to review the workload demands of the team which highlighted that additional resources were needed to support the existing workloads and undertake some of the pro-active work to further enhance the Information Management System at the Force. A business case has been prepared and presented to the Information Management Board with proposed changes to the team and the outcomes of the business case will impact on capabilities moving forward.

Finding	Recommendation	Initial Management Comments	Follow Up Result	Result / Timeframe of Risk Exposure
Policies & Procedures *Observation:* Audit reviewed the policies and procedures that are in place to govern the Information Management System in place at the Force and observed the following: The Force have an Information Assurance Framework in place that was published in July 2013. Although it was superseded by the Information Management Strategy in July 2015, it is still available on the Force intranet. The Information Management Strategy is currently not aligned to the new structure that is in place and the new Information Asset Owners that are in post following the move to the thematic model in May 2016. The Force Information Assurance Board Terms of Reference were put in place in 2012 prior to	**Priority 2** The Strategies, Policies and Procedures that support Information Management at the Force should be reviewed and updated in line with the current processes that have been adopted. The documents to be addressed are: • Removal of the Information Assurance Framework, as this was superseded by the Information Management Strategy. • A review and update of the Information Management Strategy.	Action: Review and update the Strategies, Policies and Procedures that support Information Management in line with current processes. The documents which should be addressed are: 4.1.1 Remove the Information Assurance Framework as this has been superseded by the Information Management Strategy. 4.1.2 Review and update the Information Management Strategy.	The Information Assurance Framework has been removed from the intranet. The Information Management Strategy was updated in July 2018. Since the audit visit the previous Finance Information Assurance Board has been merged with the Crime Data Integrity Board and an Information Management Board is now in place and has held three meetings during 2018. Audit were provided with the terms of reference for new Board, which shows that monitoring and oversight is included within the scope of the Board.	Recommendation Implemented.

the establishment of Information Asset Owners, Information Asset Registers and Information Risk Register and, as a consequence, requires reviewing to ensure it remains fit for purpose. It also states bi-monthly meetings should take place, however meetings are currently held on a quarterly basis. There is also a lack of clear structured performance monitoring at the FIAB meetings that take place. *Risk:* Inconsistent working practices are followed as there is a lack of clarity in the correct processes and procedures that are to be followed.	• A review and update of the Terms of Reference for the FIAB including performance monitoring.	Consideration to be given to the new structure in place and with the recommendations raised from this audit. Link this to recommendation 4.8 4.1.3 Review and update FIAB Terms of Reference to include performance monitoring. December 2016		
IAO Job Descriptions *Observation:* The Information Asset Owner role is assigned to certain job posts across the force and, in line with the new structure, these are Heads of Departments. The role of IAO's is currently documented within the Information Asset Owner Handbook however, the IAO role is not included within the job descriptions of these roles. *Risk:* Information Asset Owners are not clear on their roles and responsibilities	**Priority 3** The Job Descriptions of the posts that are to be Information Asset Owners should be updated to reflect the responsibilities and embed the importance of the role.	4.2.1 Add IAO job descriptions update as an agenda item at the November 2016 FIAB meeting and agree how best to proceed. The DCC to identify how the IAO role can be specifically identified for Police Officer roles 4.2.2 Update the Job Descriptions of the posts of Information Asset Owners to reflect the responsibilities and embed the importance of the role. The role of IAO can only be specifically identified in the Job Descriptions of the relevant civilianised roles (predominantly Heads of Departments). Information Management will provide the wording to be added and a list of roles to HR to facilitate this addition. March 2017	The Information Management Lead has worked with HR to ensure that the Information Asset Owners job descriptions have been updated to reflect their responsibilities. Audit were provided with a sample of job descriptions which clearly included information asset responsibilities.	Recommendation Implemented.

IAO Training & Handbook *Observations:* When an IAO is new to the role, a one to one meeting is held with the Information Security Officer to explain the role and responsibilities and they are provided with an Information Asset Owners Handbook. An e-learning module hosted by another Force is available, however this is not mandatory and the Force cannot monitor if this has been completed by the IAO and any of their delegates. The Information Asset Owners Handbook does not clearly document the process that should be followed by IAO's in the production and maintenance of the Information Asset Register. Whilst it provides a steer, it does not clearly state what actions are to be taken and the role the ISO plays in supporting the production and maintenance of the IAR. *Risk*: IAO's are unable to perform their job adequately in managing information.	**Priority 2** The current training offered to IAO's and delegates should be reviewed and a decision made on how to deliver initial training and refresher training to ensure the Force has appropriately trained individuals performing the IAO role. The IAO Handbook should be updated to reflect the current processes that are in place and provide clarity on the actions that IAO's need to take to produce and maintain the information asset register. A clear process should be in place so that a 'gatekeeper' is in place to monitor consistency of the register.	Action: 4.3.1: Review the current IAO training and support package in place (Nottinghamshire Police provide specific one to one sessions with all IAO's and their delegates and ongoing face to face support as well as the eLearning package provided by Lincolnshire which was agreed for regional use at the Regional Information Assurance Group) Present proposals for new and existing IAOs to FIAB in November 2016. To include relevant costing if applicable. 4.3.2: Update the IAO handbook to reflect the current processes followed and provide clarity on the actions that IAO's need to take to produce and maintain the information asset register. 4.3.3: Amend the Information Security Officer Job description to include the role of 'gatekeeper' to maintain the IA register and ensure that returns do not include missing data. This process will be included within the updated IAO handbook. March 2017	As set out in the Summary above, the Information Management Lead has recently presented a business case for a significant increase in staffing within the team to allow a more proactive approach to information management. As a consequence, there has been limited change in the training approach to IAO's at present. However, the business case currently been considered will include additional staff who will act in a business partner model to provide support, guidance and training to IAOs. Due to resources the IAO handbook has not been updated. The job description of the Information Security Officer has been updated to clearly include the 'gatekeeper'.	Partially Implemented.
List of IAO's and Delegates *Observation:* The Information Security Officer holds a list of all IAO's, however there is no complete list of all IAO's and their delegates. Whilst there are 23 information asset owners on the list held by the Information Security Officer, there are a further 73 delegates listed within the overall information asset register. *Risk:* The Information Management team cannot operate efficiently if the delegates are unknown	**Priority 3** The Information Management Team should hold a complete list of Information Asset Owners and delegates and this should be published so staff are aware of the right contacts should they need to raise an issue.	Action: Complete a list of Information Asset Owners and delegates. Publish on the Force intranet so that staff are aware of the key contacts for information assets. November 2016	A list of Information Asset Owners and delegates is included in the updated Information Asset Strategy. The Strategy is not currently published on the Force intranet due to a new intranet site being launched at the Force in the next few months. The Information Management Team will upload it when the new site is launched.	Recommendation Implemented.

Completeness of the Information Asset Register *Observation:* Audit reviewed the current version of the Information Asset Register and found missing information. Of the 473 Information assets listed: • 132 had no asset id number assigned to it; • 46 had no department or division listed; • 30 had no asset description completed; • 22 has no Information Asset Owner listed; • 132 had TBC under the delegate listed; • 14 had no business impact level completed; • 219 did not state sensitivity of information; • 31 did not list the format that the information was held in; • 42 did not list the location of the asset or was listed as unknown location; • 56 did not have a point of contact completed; and • 61 did not state if the information was shared. *Risk*: The Force have not clearly identified the key information around the assets that have been registered and therefore may not manage their information in line with legislation.	**Priority 2** IAO's should be tasked to complete the missing Information.	Action: Contact the IAOs and update the Information Asset register with the identified missing information. Cross ref with recommendation 4.3.3: Amend the Information Security Officer Job description to include the role of 'gatekeeper' to maintain the IA register and ensure that returns do not include missing data. This process will be included within the updated IAO handbook. November 2016	The Force have appointed a new Information Security Officer since the last audit and they have developed a new format of the information asset register that includes links to the records management. However, this is still to be completed and fully populated with the information assets held on the current register. The OPCC has recently updated its Information Asset Register as part of the preparations for GDPR. Work still needs to be completed on populating the register in a consistent format.	Partially Implemented.
Format of the Asset Register *Observation*: The Information Management Strategy states the Force will maintain an information asset register that will capture location, format and review, retention and disposal (RRD) practices. The current format of the Information Asset Register does not make a reference to the RRD practices of each asset. *Risk:* The Force breach legislation by keeping information that it should not.	**Priority 2** The Information Asset Register should be updated to include review, retention and disposal details.	Action: Update the Information Asset Register to include a review, retention and disposal column. A retention schedule is in place. November 2016	As referred to above, a new information asset register format has been drafted. This has clear links to the records management team so that marking and retention dates can be included.	Recommendation Implemented.

Information Risk System *Observation:* The Force has an Information Risk Management Strategy in place. However, a review of this against the current processes followed and the knowledge of the responsibilities of key parties highlighted inconsistencies. The role of the Information Asset Owners in identifying risks, adding risks to the register and taking mitigating actions is not clearly documented or understood by the IAO's. Whilst an information risk register is in place, it does not provide the Force with assurance that the risks are being appropriately managed. The risk register has an IAO listed for each risk, however it does not clearly state that they are the risk owner and that they are responsible for managing the specific risk. Moreover, the risk register simply states risk mitigation is the information asset owner's responsibility. It does not document the controls in place and the mitigation actions that should be taken to manage the risks that have been identified. In addition, there was no evidence that the risk register had been reviewed or updated for six months. The Information Risk Register currently has no clear links to the Information Asset Register and therefore asset owners are not aware of which risks are relevant to the assets they look after. *Risk*: The Force does not manage its information risks effectively, leading to breaches in legislation incurring financial and reputational damage.	**Priority 1** The Information Risk Management system in place at the Force needs to be reviewed, updated and implemented. This should include, but not be limited to, the following: • An update to the Information Risk Management Strategy. • The responsibilities of IAO's in relation to identifying and managing their risks needs to be clearly communicated. • The process for adding risks, closing risks and updating risks to the information risk register needs to be agreed upon and formally communicated. • The format of the risk register should clearly include Risk Owners, the risk mitigation actions that are in place, confidence levels of the actions in mitigating the risks and timescales for completion. • The process for regular monitoring of the Information Risk Register should be established. • There should be clear links between the information risks identified and the information assets the Force holds.	Action: Review, update and implement the Information Risk Management system. This should include, but not be limited to, the following: • An update to the Information Risk Management Strategy. • The responsibilities of IAO's in relation to identifying and managing their risks needs to be clearly communicated. • The process for adding risks, closing risks and updating risks to the information risk register needs to be agreed upon and formally communicated. • The format of the risk register should clearly include Risk Owners, the risk mitigation actions that are in place, confidence levels of the actions in mitigating the risks and timescales for completion. • The process for regular monitoring of the Information Risk Register should be established. • There should be clear links between the information risks identified and the information assets the Force holds. March 2017	The Information Risk Strategy has been superseded and the approach that is now taken to managing information risks is included as part of the Corporate Risk Management approach. As a consequence, an information risk register is held alongside other departmental risk registers and risks are now reviewed on a monthly basis with the Risk Management Officers, with cyclical reviews by the DCC. The responsibilities for managing information risks are included within the information risk register, with risk owners assigned to the risks detailed and associated risk mitigation actions. These are reviewed monthly. It was noted from a review of the information risk register that the previous Head of Corporate Services is still listed as a risk owner, but has left the organisation so it does require updating. The format of the information risk register is aligned with the other departmental risk registers at the Force. The alignment to the risk register and the information asset register will be completed once the information asset registers has been fully completed (see comments above).	Partially Implemented.

Audit Role *Observation:* The new structure of the Information Management Team includes the use of an Information Auditor. This resource is to be used to provide assurance to the Force that they are compliant with legislation in the management of information. However, at present there is no formal documentation of the role that information audit plays in the management of information at the force, with no reference to the role within the Information Management Strategy. *Risk*: The Force do not effectively utilise the information audit resource to provide assurance.	**Priority 2** Management should decide upon the role that Information Audit is to play within the Information Management System in place and clearly document this.	Link this to 4.1.2 Action: Review and update the Information Management Strategy. Consideration to be given to the new structure in place and with the recommendations raised from this audit. December 2016	A review of the Information Asset Strategy confirmed that the role of audit is listed under the information management roles and responsibilities. This being: *'The main purpose of the audit function is to provide the organisation with an independent assessment and appraisal of compliance with the Data Protection Act 2018. Business areas originally identified in the Management of Police Information Guidance as being the most significant for policing purposes have been included as the 'core' areas for audit. E.g Crime, Intelligence and Public Protection.'*	Recommendation implemented.
Audit Process *Observations*: An audit schedule is presented to the FIAB for approval by the Information Auditor which is based on HMIC recommendations, current issues and previous audits. The audits are completed and then reports issues directly to information asset owners. At the FIAB meetings an update on the progress of the schedule is discussed. However, there is a lack of clarity of the audit process, with no timescales for the issuing of audit reports and monitoring of the audit outcomes and recommendations being completed. *Risk*: The outcomes of information audits are not embraced and issues identified are not rectified leading to the Force being exposed to breaches of legislation.	**Priority 2** The audit process should be clearly documented and communicated to Information Asset Owners. This should include, but not be limited to, the following: • Timetables for scheduled audits, with agreement of audit schedule and fieldwork. • Timetable for issuing of draft reports and expected responses to findings. • Distribution lists for final audit reports. • Follow up of audit recommendations. • The monitoring of actions to implement audit recommendations. Summarised feedback at FIAB of completed audit reports.	Write separate policy and procedure documents to include, but not be limited to, the following: • Timetables for scheduled audits, with agreement of audit schedule and fieldwork. • Timetable for issuing of draft reports and expected responses to findings. • Distribution lists for final audit reports. • Follow up of audit recommendations. • The monitoring of actions to implement audit recommendations. • Summarised feedback at FIAB of completed audit reports. When complete communicate to IAO and publish on the intranet / library March 2017	An agreed annual audit schedule has been put in place and the audit work that is completed is now reported to the Information Management Board as a standing agenda item. Moreover, the recommendations raised by the audits are now included on the Force tracker, 4action, so that they are tracked alongsid	