Appendix D:

JAEC Update: Audit of Constabulary Information management and security arrangements

Introduction

1.1 This report has been produced at the request of the Joint Audit and Ethics Committee on 11 December 2017.

1.2 It provides an update for members on the Audit findings that were originally reported in 2015-16 following our initial review of Constabulary Information management and security arrangements, the further work that was conducted during 2016-17 and our final 'follow up' review that was completed earlier this financial year.

Refer Appendix 1

Previous audit conclusions

1.3 At the time of our original examination of the Constabulary Information management and security arrangements (March 2016), we provided limited assurance regarding the adequacy of the arrangements in place. In particular our audit identified a range of weaknesses in the governance of information most notably a complete and accurate information asset register and the absence of an information risk register.

Refer Appendix 2

1.4 Further work was conducted in May 2017 to determine the progress made by the Constabulary and at that time we provided substantial assurance over the adequacy of the arrangements in place. A number of actions were still ongoing, and in particular the information management audit plan to ensure compliance with MoPI and APP had only been partially completed.

Refer Appendix 3

1.5 In November 2017, in accordance with the Public Sector Internal Audit Standards, we sought further assurances from the Constabulary regarding the progress made in addressing the actions previously noted as partially completed.

1.6 Whilst an assurance opinion was not appropriate, we reported to the JAEC that management were progressing agreed actions and explanations had been provided regarding the delays in implementation. In particular we referenced the fact that the MoPI audit resource had been diverted into ensuring that the Constabulary was ready for the introduction of the General Data Protection Regulations in May 2018 and the new Data Protection Bill.

1.7 The table below demonstrates numerically the actions initially raised in March 2016 that were ongoing as at November 2017:

Risk	Number	Implemented	Ongoing
High	2	1	1
Medium	12	10	2
Low	2	2	0
Total	**16**	**13**	**3**

Going forward

1.8 The actions currently shown as 'ongoing' in the above table relate to the following areas:

- The need for ensuring compliance with mandatory information assurance training; and
- Population of the Information Management risk register and the periodic assessment of all systems and processes that deal with sensitive information.

1.9 Our recent liaison has therefore confirmed that progress continues to be made by the Constabulary in addressing the areas for improvement originally identified, and which are still relevant for progression. A draft programme of work is also currently under development for the Information Assurance audit team for 2018/19.

Appendix 1: Current status of agreed actions

Original agreed actions following our work in March 2016	Update reported as at May 2017 and further actions noted	Status reported as at November 2017	Future activity
POLICY FRAMEWORK AND GOVERNANCE **A1 – Medium risk (Implemented)** The suite of policies and supporting procedures should be reviewed to identify any areas where additional policy or procedural guidance is required. An action plan with agreed timescales should be agreed to address any gaps and ensure there is adequate coverage of all information management and security risk areas. **A2 – Medium risk (Implemented)** The format and content of all information management and security policy documents should be reviewed to ensure they contain achievable standards and accurately reflect the Constabulary's information management and security objectives. This should include clarification of the governance arrangements for approval and review of all policies and procedures. The documents would be improved by a better	The Constabulary has taken a number of actions to align their policies, procedures and arrangements to MoPI principles, including: • The development of a Records Management Policy Statement and Retention/ Disposal Schedule; • Establishing an information management audit plan that identifies the legislation to be followed, risk assessments completed, key risk areas by score, and reviews required; • The permanent appointment of two MoPI auditors to implement the above plan; • Reporting MoPI requirements, developments and audit at all meetings of the Information Governance Board (IGB). Six of the nine policies reviewed as part of this review did not include a version control matrix due to an update to the policy templates issued by Corporate Development.	The new intranet facility was implemented during the summer of 2017 and all polices are available within. Archived polices are saved and can be obtained from Corporate Development, if required. **(Implemented)** We have received assurances that the Information Security Policy and the Information Governance Board terms of reference have both been reviewed and updated to ensure they are consistent. **(Implemented)**	Regarding the information management audit plan, whilst the main systems and key areas have been identified and risk assessed, completion of the necessary compliance work was limited during 2017/18 as the audit team were involved in the preparations for the General Data Protection Regulations (GDPR) and the forthcoming new Data Protection Bill. This included a review of contracts with third party processors, a review of force polices and further development of the Information Asset Owner register. A draft audit programme is being developed for 2018/19.

Original agreed actions following our work in March 2016	Update reported as at May 2017 and further actions noted	Status reported as at November 2017	Future activity
document and version control and a revision history. **A6 – Medium risk (Implemented)** All guidance issued should be regularly reviewed with review schedules and responsibilities agreed and documented within the Constabulary's policy and procedural documentation. **A3 – Low (Implemented)** The Terms of Reference for the Information Governance Board and the definition of all roles in the management of information should be collated into a single definition in one framework document.	It is understood that the introduction of a new Constabulary Intranet facility in May 2017 will address this issue by providing an improved search facility that will only return the latest version of a policy. Minor differences were noted in the documented role of the IGB and as a result, the following additional low risk action was raised: *The Information Security Officer and Information Assurance Manager will review/ update the Information Security Policy and IGB terms of reference documents to ensure that they are consistent.*		
TRAINING **A7 – Medium (Implemented)** A formal training strategy should be developed and adopted to develop an information management and security culture in line with the Information Management Strategy. **A5 – Medium (Ongoing)**	A draft training plan has been developed that will be presented at the meeting of the IGB in May 2017. In addition to the framework of policies and procedures, the new Intranet facility due in May 2017 will incorporate presentations and	CPD events with Information Asset Owners have commenced and include preparations for GDPR and DPA reform, which will identify possible risks for inclusion in the	Liaison with the Information Assurance manager has confirmed that the need for mandatory training is recognised in the GDPR/ DP Reform action plan. Training packages are currently being

Original agreed actions following our work in March 2016	Update reported as at May 2017 and further actions noted	Status reported as at November 2017	Future activity
A schedule of periodic testing should be considered, at least on a sample basis, to ensure that the mandatory training is being carried out by all personnel. **A4 – Medium (Implemented)** Up to date guidance for Information Asset Owners (IAOs) should be made available along with access to appropriate training as and when required.	guidance on information management and security. The annual Information Management audit programme allows the effectiveness of existing training and guidance to be established through the completion of risk assessments and dip sampling of compliance with the Data Protection Act, ACPO guidance, APP and HMIC requirements.	Information Management risk register. **(Implemented)**	developed nationally, which will be rolled out once available. Corporate training records will be maintained in order to enable attendance to be monitored.
INFORMATION RISK **A8 – High (Ongoing)** The Information Risk Register should be set up as soon as possible along with a process to escalate or transfer information risks to corporate and departmental risk registers as appropriate. Reporting arrangements should be agreed with the SIRO and the Information Governance Board that are in line with the established corporate risk management process. **A9 – Medium (Implemented)** The Privacy Impact assessment (PIA) process should continue to be	The development of an information risk register for the Constabulary was ongoing at the time of the audit. The Information Assurance Manager is seeking to fully populate the risk register by the end of 2017 in preparation for the implementation of the data protection legislative regime. The Constabulary has developed and issued guidance on when and how to carry out a PIA and a template is in place to facilitate the process. These are available in the Constabulary's document store.	The Information Management risk register has not yet been populated although the risks associated with the introduction of the GDPR and the Data Protection Bill are recognised on the corporate risk register. **(Ongoing)**	Liaison with the Information Assurance manager has confirmed that it is anticipated that the information management risk register will be updated in readiness for the April meeting of the Information Governance Board.

Original agreed actions following our work in March 2016	Update reported as at May 2017 and further actions noted	Status reported as at November 2017	Future activity
promoted and enforced across the Constabulary to ensure assessments are carried out where required. **A10 – Medium (Ongoing)** A risk assessment of all systems and processes that deal with sensitive information should be carried out on a regular basis as part of the information risk management process.			
INFORMATION ASSET MANAGEMENT **A11 – Medium (Implemented)** An up to date information asset register needs to be developed and maintained to identify information asset owners and support the information risk management process. **A12 – Medium (Implemented)** A formal project should be instigated to manage the roll out of the new protective marking scheme in accordance with national guidance and also to ensure the classification	The Information Asset Register records detail of the Constabulary's IAOs including the systems they own and their contact details. A significant exercise was undertaken during 2016 to ensure the register is up to date. The Force Records Manager, appointed in 2016, is now responsible for maintaining the register. A process has been established with ICT to ensure that the Records Manager and Information Security Officer are informed of any new systems. Action is being or has been taken to promote the GSC. Including the following:	N/A – no specific actions identified for follow up	An audit of compliance with retention schedules was completed during 2016, which led to further engagement with business areas and development of an updated retention schedule for the Constabulary in December 2017.

Original agreed actions following our work in March 2016	Update reported as at May 2017 and further actions noted	Status reported as at November 2017	Future activity
is implemented across all systems. **A13 – High (Implemented)** The audit against retention schedules should be carried out as a matter of urgency to ensure the constabulary is complying with MoPI requirements. Any risks identified from the work should be managed and prioritised accordingly.	• The introduction of a senior manager approved GSC policy since August 2016; • The planned inclusion of a dedicated page on the new Intranet facility due in May 2017; • The planned publication of an aide memoir; and • The provision of a training package.		
SECURITY INCIDENT MANAGEMENT **A14 – Medium (Implemented)** The Constabulary should agree a revised security incident procedure that includes a clear definition of how an incident should be responded to and investigated including the collection and preservation of electronic evidence. **A15 – Low (Implemented)** The existing incident reporting procedure should be reviewed with the objective of introducing a single reporting point thereby removing the	The Constabulary has an up to date, detailed Information Security Incident Reporting procedure. The Information Security Officer demonstrated on site how a security incident would be dealt with, using a loss of a device as a common example. Full operation of the security incident procedure was not tested as part of this audit review.	N/A – no specific actions identified for follow up	Our current discussions have confirmed that going forward a key pressure will be in ensuring compliance with the requirement to report Data Protection breaches to the ICO within the 72 hour window.

Original agreed actions following our work in March 2016	Update reported as at May 2017 and further actions noted	Status reported as at November 2017	Future activity
opportunity for incidents to be reported in the wrong manner and to help encourage incident reporting.			
INFORMATION SHARING **A16 – Medium (Implemented)** The audit of information sharing agreements should be carried out in accordance with the audit plan to ensure agreements have been established where required.	A review of ISAs was scheduled. The terms of reference for the review has clearly and appropriately defined the aims of the review. It includes a review of the present ISA template and guidance against the Information Sharing APP and revised national model template. Also, where access to Force systems has been provided to third party agencies, the review will establish whether a suitable ISA has been established.	N/A – no specific actions identified for follow up	This initial piece of work was completed in September 2017.

Appendix 2: Extracts from our final report - Information Management and Security – March 2016

Overall Assessment

1.1 We have completed an audit to assess the adequacy and effectiveness of the controls in place to ensure that there is no unauthorised access to or disclosure of sensitive data, particularly where the Constabulary works in partnership with other organisations.

Audit opinion

1.2 Based on our review we can only provide limited assurance over the Constabulary's information management and security arrangements at this time. However, we recognise the ongoing efforts to improve the situation and we have found examples of good practice and a commitment to improve and ensure the Constabulary's compliance with MoPI and APP guidance.

Significant findings

1.3 We have recognised throughout this audit that the personnel we have dealt with are fully aware of the weaknesses that exist and the actions needed to address them. Furthermore we have seen that there is obvious support and oversight from the SIRO and the Information Governance Board.

1.4 However, our audit has identified a range of weaknesses in the governance of information most notably a complete and accurate information asset register and the absence of an information risk register. These are fundamental components for effective information management.

1.5 The policy framework is being refreshed and whilst we feel there are still areas for improvement it does represent a positive step.

1.6 The limited centralised information management resources are being improved with the planned appointment of a records manager and two temporary MoPI auditors and the recent appointment of a deputy Information Security Officer. Despite this, the role of the information asset owners across the Constabulary is vital and engagement with these key personnel needs to be improved.

1.7 It is difficult to assess at this stage if the additional resources being provided will be sufficient but it is crucial to ensure the additional resources are focused on key areas of risk and suitably managed to get the best value. To achieve this a clear programme of work should be defined as soon as possible to facilitate the prioritisation of the projects necessary to fully realise the Constabulary's objectives and information management strategy.

1.8 Although not specifically addressed in our detailed findings it is important that, as the Constabulary's information management and security framework is developed, consideration is given to how compliance with the framework will be enforced with the resources available.

Appendix 3: Extracts from our final report - Information Management and Security – May 2017

Overall assessment

1.1 The main emphasis of the audit has been to review the progress made by the Constabulary in implementing the actions agreed in the 2015/16 report issued in March 2016, focussing on the current framework of information security policies, related procedures and guidance.

Audit opinion

1.2 The audit work we have undertaken allows us to provide **substantial** assurance over the adequacy of the Constabulary's information management and security framework.

1.3 Actions have been taken since the last audit to improve the arrangements in place, in particular the steps taken toward compliance with MoPI (Management of Police Information) and APP (Authorised Professional Practice). Whilst significant progress has been made, a number of the actions instigated to ensure full compliance are still ongoing. For example, the information management audit plan has only been partially completed. The Constabulary through the Information Security Officer, Information Assurance Manager and its Information Governance Board (IGB) are fully aware of these areas and the actions being taken or planned for 2017.

Significant observations

1.4 Good practices are in place. These include:

- Clear support and oversight of information management and security from the Senior Information Risk Owner (SIRO) and IGB;
- The establishment of an up to date framework of information management and security policies;
- The maintenance of an Information Assets Register that records the Constabulary's Information Asset Owners including the systems they own and their contact details; and
- The establishment and development of a risk based annual information management audit plan.

1.5 There are areas, however, where action is ongoing. Most significantly:

- Whilst risk assessments have been undertaken for all areas detailed in the information management audit plan, the compliance testing completed was limited. This is expected to be addressed during 2017/18 when MOPI auditors are more able to focus on completion of the plan following permanent posts being established which will focus on data protection/ information compliance audits;
- Non-compliance with the framework of information management and security policies will be identified as the information management audit

plan is completed. This will allow any issues to be considered and corrective action to be taken;

- The development of an information risk register is due to be completed in 2017; and
- A new Intranet facility for the Constabulary is due in May 2017. This will allow the information management and security policies, related procedures and guidance to be made available to staff in full. The intended improvements in the search function will provide a significant enhancement on the current facility that is in use.

1.6 Our work did identify one area where, although considered low risk, improvement could be made to the existing policies and procedures:

- Roles and responsibilities detailed in the Information Governance Board terms of reference were not consistently represented in the Information Security Policy. This was raised in the March 2016 report, and the Information Security Officer and Information Assurance Manager agreed to review the documentation again to clarify.