BRITISH TRANSPORT POLICE

Report to:	**Audit & Risk Committee**
Agenda item:	**10**
Date:	**25 November 2015**
Subject:	**Information Management Update**
Author:	**Helen Edwards/Director of Capability and Resources**
Sponsor:	**Director of Capability and Resources**
For:	**Information**

1. PURPOSE OF PAPER

1.1. To update the committee on Information Management within BTP. The Force provided a comprehensive update to the October Audit and Risk Committee. This update covers recent developments since that brief.

2. EXPLANATION OF TERMS

2.1. This paper refers to various physical records at various states of non-compliance, the Management of Police Information (MOPI) retention guidance regulations, and nominals.

2.2. The table below explains the different MOPI groupings.

Group	Definition	Undetected	Detected
MOPI Group 1	Serious violent and sexual offences (like murder and rape)	Retained for 100 years from date of offence. Reviewed every 10 years	Retained for 100 years from date of birth of youngest offender. Reviewed every ten years
MOPI Group 2	Less serious violent and sexual offences (like ABH and sexual assaults)	Retained for 10 years from date of offence and then a senior officer to review	Retained for 10 years from date of offence and then senior officer to review
MOPI Group 3	All other offences that are non-violent and non –sexual (like fraud, theft, byelaw offences)	Retained for 6 years from date of offence and then senior officer to review in case there is a policing purpose to retain	Retained for 6 years from date of offence and then senior officer to review in case there is a policing purpose to retain

2.3. Nominals: A nominal record is one that relates to, consists of or is assigned a person's name. When creating a nominal record, it should contain, as a minimum, one of the following: forename / family name / partial name / nickname / alias. A description has to include a name in order to create a nominal record. Other desirable basic fields to add to a person record are: age (date of birth) / sex / colour / ethnic origin / height.

3. GOVERNANCE AND ASSURANCE

3.1. The Force has rewritten and issued the IM Strategy and supporting handbooks.

3.2. Governance**.** The governance framework was described in detail in the information strategy. It is summarized in the table at Annex A.

4. IM RESET

4.1. The Force is mid-way through a reset of information compliance across all functions, divisions and departments. The reset:

4.1.1. Captures information inputs and outputs and documents both physical and electronic records management processes, including retention periods and responsible owners for all areas of work.

4.1.2. Focuses on the suite of IM documentation including strategy, policies, procedures, guidance and newly published handbooks ensuring they have been circulated and that teams are assessing their compliance against these.

4.1.3. Captures where information sharing takes place identifying points of contact and ensuring robust processes to safeguard data.

4.1.4. Documents who owns information assets to ensure confidentiality, integrity and availability of data

4.2. The reset will be completed by **January 2016**.

5. TRAINING

5.1. Training is in place for all staff (IM NCALT package) and specifically for those responsible for the physical archiving process and the use of Cycmopa the BTP physical records archiving database. A CycMoPA user guide has been created and published alongside two handbooks on how to manage both end of life records and live records held at a police station. All Cycmopa users will be trained by **January 2016**.

6. IM ASSURANCE

6.1. The IM Assurance regime has been reset. Four Audit and Advisory Officers are in place within IM and will embark on an audit schedule starting in January 2016, when the reset phase has been completed. The main functions, divisions and departments will be subject to a formal Ofsted style audit over the following 12 months. Each audit result and report will be submitted to the Information Governance Board, the business area lead and the Chief Officer Group. Audits will be prioritised depending on the baseline findings ensuring areas of weakness are addressed at the earliest opportunity.

6.2. The main business areas will be audited against IM compliance between **January and December 2016.**

7. UNSTRUCTURED DATA PROJECT

7.1. The project has successfully delivered a range of controls relating to e-mail management and the management of personal and departmental drives. There are now clear retention periods set for e-mails relating to inboxes and the archive, with all functions automated. Guidance has been issued covering the correct process for storing departmental information which includes folder

structures, the allocation of a responsible owner and the process by which the Audit & Advisory Officers will check compliance.

7.2. Additionally a business case will be submitted to Service Improvement Board in December outlining the strategic options for an electronic document records management system (EDRMS).

8. PSN REMEDIAL RISKS

8.1. Interim accreditation has been given for BTP to connect to the new Public Service Network (PSN), with full accreditation dependant on the successful completion of projects to address areas of non-compliance. Progress against project milestones is reviewed at fortnightly IGB meetings and BTP are on track to deliver against the plan by the scheduled dates in 2016. Monthly updates are provided to the National Accreditor at the end of every month and all projects are currently on track.

9. MANAGEMENT OF POLICE INFORMATION (MOPI) SELF ASSESSMENT

9.1. The Audit and Compliance Team are working with Information Management to carry out a self-assessment against the requirements of the Authorised Professional Practice (APP) on MoPI, in order to comply with a request from Her Majesty's Inspectorate of Constabulary (HMIC). Areas of non-compliance currently exist relating to existing legacy systems and the inability to apply groupings to records and to auto weed.

9.2. It is anticipated that the introduction of the Niche integrated records management system for operational policing will fill the gaps. The self-assessment will assure that plan and identify any further issues to address in order to achieve full compliance with the APP. The self-assessment will be completed and reviewed at IGB prior to submission to the Integrity and Compliance Board (ICB).

10. OPERATION CANBERRA

10.1. In January 2015, the Force had some 31,000 boxes of physical records stored at IRON MOUNTAIN. A smaller amount were stored locally 'on area' or held securely by other storage providers.

10.2. Of the 31,000 boxes, nearly 20,000 were not indexed, nor were the files held on CycMOPA. In effect, the contents of the boxes were not known and not searchable. These were known as the *'10,000 boxes'* and were the original focus of Op CANBERRA. These have now all been retrieved and reviewed. The majority of the contents were destroyed. What remains is in the process of being re-archived. This will be complete by the **end of 2015**.

10.3. The remaining 11,000 boxes are indexed and the files are held on CycMOPA. The files are individually searchable but the boxes are mixed. To appropriately review and delete files that should not be retained, all the boxes must be retrieved. This is ongoing. The Operation is receiving 500 boxes per week into Caledonian Rd, delivered on 13/14 pallets. The pallets are managed by a group of experienced Police Officers and staff who sift and sort the files into categories and undertake an initial triage operation. The boxes and their contents are then examined by a separate group of staff who enter the details of the retained files onto Cycmopa. Approximately 70% of what comes in goes back out as waste.

11. RISKS

11.1. The risks as a result of the ongoing IM situation are:

11.1.1. Retention of unreferenced material. This refers to the material that was retained after the review of the '*10,000 boxes'* and which still awaits re-archiving on CycMOPA. The Force is not in contravention of DPA but the records are not logged. In the event of a subject access request the

remaining records would need to be worked through manually. This will be addressed by **January 2016.**

11.1.2. Retention of material beyond authorized time limit. This refers to the 11000 boxes of mixed files. The MOPI 3 files are overdue weeding. There is no risk and harm issue with these records which can be accessed. This is being addressed as a priority by Op CANBERRA. This will be complete by **29 February 2016.**

11.1.3. FIS Back Record Conversion and Nominal Creation. This refers to FIS records where an individual is linked to a single piece of information. Some of these relate to a case, others are merely information. These records must be reviewed and where relevant a nominal will be created. This work is paused whilst staff focus on the physical records. The FIS back record work will be complete by the introduction of Niche in **mid-2016.**

11.2. **Sub-optimal exploitation of information**. Beyond the legal requirement there is an issue with the operational and business impact arising from sub-optimal information management. There are three elements:

11.2.1. Niche/ISP. Niche and ISP require a high level of cleansed data. This is being addressed by the ISP's data migration strategy. This will be addressed by **mid-2016.**

11.2.2. Non-ISP Data. This is being reviewed by the Information Governance Board to ensure that due consideration is given to data which whilst not required by Niche, may be affected or become legacy because of Niche.

11.2.3. Force-wide IM. The IM reset is overhauling the general skills and processes by which information is managed across the Force. The target date is **January 2016.**

12. INFORMATION COMMISSIONER'S OFFICE

12.1. The Director of Capability and Resources and the Head of Information Management met with representatives from the Information Commissioner's Office on the 20th of October to discuss Operation Canberra and how BTP were improving the management of information.

12.2. During the meeting a briefing was given on the process employed to review the *10,000 boxes*. A range of current privacy matters were also discussed ranging from strategic work by National Police Chief Leads on Body Worn Video Cameras to retention periods for biometrics. Following the conclusion of the meeting the representatives stated they felt assured with our progress and plans and as a result would not be progressing the matter any further.

12.3. The Force has accepted an invitation for an ICO advisory audit in due course and will meet the ICO Team as part of their engagement strategy quarterly.

13. RECOMMENDATION

13.1. That the Committee note the contents of this paper

Annex A: Governance Framework