BRITISH TRANSPORT POLICE

Report to:	**Audit & Risk Assurance Committee**
Agenda item:	
Date:	**12 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 last Audit and Risk Committee. This update covers recent developments since that brief.

2. UPDATE

2.1 The Force has rewritten and issued the IM Strategy and supporting handbooks. At the last committee meeting a question was asked in regard to the governance framework and the risk carried in information management.

2.2 Governance**.** The governance framework was described in detail in the information strategy. It is summarized in the attachment.

2.3 Risks. The risks present as a result of the ongoing IM situation are detailed below with completion targets:

2.3.1 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 is being addressed by Op Canberra and will be complete by December 2015. Ongoing training for all Cycmopa administrators will conclude in December 2015.

2.3.2 Retention of material beyond authorized time limit. This refers to some 8,500+ boxes which are held at IRON MOUNTAIN. These boxes are correctly indexed (by box) but contain mixed MOPI 1, 2 and 3 files. The MOPI 3 files are overdue weeding. There is no risk and harm issue with these records which can be accessed. The '8,500 boxes' are being addressed as a priority by Op Canberra This will be complete by 29 February 2016.

2.3.3 FIS Back Record Conversion and Nominal Creation. This refers to FIS records for single entity nominals (ie an individual where there is not more than a single piece of information). The work is to create nominals where applicable. This will ensure full compliance with PND. This work is paused at present to concentrate on the re-archive work. It will be completed by the introduction of Niche in mid-2016.

2.3.4 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:

2.3.4.1 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.

2.3.4.2 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 affected or become legacy because of Niche.

2.3.4.3 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.

3. IM RESET

3.1 The Force is mid-way through a reset of information compliance across all functions, divisions and departments. Target date is January 2016. The reset:

3.1.1 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.

3.1.2 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.

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

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

4. IM ASSURANCE

4.1 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 addresses at the earliest opportunity.

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

5. OPERATION CANBERRA

5.1 OP Canberra has now recalled over 22,000 boxes of material from archives. As of today, 8700 boxes remain in storage with Iron Mountain and will be extracted over the next 18 weeks. Once this operation has concluded all legacy boxes previously stored with Sergeants, Wincanton and Iron Mountain will have been subject to a RRD process. The planned end date for this operation is the 29th February 2016.

5.2 Since July 2015, 1140 boxes have been returned to Iron Mountain for storage, these boxes form part of account EL622, which has been set up to record the files/boxes created as a result of OP Canberra. On average the team is processing on Cycmopa approx.150 boxes per week.

5.3 The Operation is receiving 500 boxes per week into Caledonian Rd, delivered on 13+ 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 the BTP document record management system known as Cycmopa. Approximately 70% of what comes in goes back out as waste.

5.4 40 staff work on this operation made up of Police Officers, Police Staff, Agency Staff and temporary staff from B and A division. The Operation is also delivering training for all administrative staff across the force. Part of this team were also creating nominal for uploading onto PND. This work has been frozen whilst the surge of boxes is managed albeit nominals for all detected MOPI 1 files are created as part of the Cycmopa exercise.

6. PHYSICAL RECORDS MANAGEMENT

6.1 All archiving as part of business as usual has been suspended for a short time while the Force trains all staff involved in the physical archiving process. The CycMoPA Administrator has been accredited to deliver training on the use of the system and has combined this with practical training on how to complete the entire end to end process. Training is ongoing and all users will be trained by December 2015.

6.2 A CycMoPA user guide has also been created and published alongside two handbooks on how to manage both end of life records and live records being managed at a police station.

6.3 Early in the New Year all staff involved in the process will have been formally trained, supported by up to date documentation and with an audit process supplied by the Audit

and Advisory Team. All records held in Iron Mountain will be correctly stored and weeded.

7. INFORMATION COMMISSIONER'S OFFICE

7. 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. 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. 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.

8. UNSTRUCTURED DATA PROJECT

8.1 The project has successfully delivered a range of governance and 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.

8.2 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).

9. PSN REMEDIAL RISKS

9.1 Interim accreditation has been given for BTP to connect to the new Public Service Network (PSN), with full accreditation dependent on the successful completion of projects to address areas of non-compliance. Progress against project milestones are 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.

10. MANAGEMENT OF POLICE INFORMATION (MOPI) SELF ASSESSMENT

10.1 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. 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 gaps 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).

Attachment

The flow chart illustrates the major points of assurance and governance for IM. Within the Force the Chief Constable leads IM as Data Controller supported by DoCR as SIRO and the Head of IM. That said, the IM strategy makes clear that IM is the responsibility of every line manager and individual who uses information. Within the BTPA, the Chief Executive serves as an accounting officer in the Information Assurance role.