RESTRICTED

Information Management

Information Audits

Essex Police's long-term vision for its information is: to create, obtain and use information of the necessary quality and completeness to best enable the force to achieve its business needs; and to handle that information appropriately.

Author: Andy Begent, Head of Information Management
15th October 2010
V01_2
Approved at Information Management Board on 14th October 2010

---

1 Introduction

1.1 Essex Police's Information Management Compliance Testing Strategy 2010-2012 requires that a programme of compliance testing work should be produced for acceptance and endorsement at the Information Management Board (IMB). This document has been produced to satisfy that requirement.

1.2 Compliance Testing is designed as a response to the following information risks:

- 1.2.1 Inappropriate access to information;
- 1.2.2 Inappropriate use of information;
- 1.2.3 Inappropriate sharing of information;
- 1.2.4 Failure to provide information;
- 1.2.5 Poor quality of information (inadequate, inaccurate, misleading, irrelevant etc);
- 1.2.6 Loss or misplacement of information;
- 1.2.7 Destruction of, or damage to, or denial of access to information;
- 1.2.8 Lack of space to store information;
- 1.2.9 Other breaches of information security.

2 Programme of Work

2.1 In view of the current uncertainty over the future structure and resourcing of Essex Police the programme of work outlined below comprises of a consolidation of activity already in existence or planned.

2.2 'Traditional' Data Protection audits of Bichard Systems are no longer seen as appropriate with the arrival of the Data Quality & Profiling Tool within the next six months. This 'gap' is seen as presenting an insignificant change from the existing risk level.

2.3 Data on PNC will still need to be looked at where there is a risk of arrest (and therefore inappropriate arrest on incorrect information). The only exception to this is disqualified driver information which, subject to a national decision by ACPO, is likely to be removed from the PNC at a future date. Meanwhile, another traditional audit – PNC Warning Signals – has been dropped as mechanisms within PNC Bureau mean these are reviewed, while they invoke no power of arrest.

2.4 It is recognised that some of the risks identified above will not be addressed by the programme.

2.5 The proposed programme of work can be found overleaf:

Title	Comments	Timescale	To be conducted by
Email	Designed to deter and identify inappropriate use of the email system i.e. - is contrary to P60/06 (and G0802) and the forthcoming Email System Operating Rules. Will include the following strands to be implemented in stages: • Audit of top ten users (to identify excessive or inappropriate use); • Audit of emails marked as CONFIDENTIAL (to test inappropriate GPMS marking); • Audit of attachments sent to non .pnn accounts (to test inappropriate circulation of sensitive information). In addition: • Lists of users' activity by volume will be provided by Audit & Inspection to Districts for their own action as they see fit; • ITD will monitor mailbox sizes and instigate appropriate action on an ad-hoc basis.	Monthly commencing November 2010	Audit & Inspection
Internet	Designed to deter and identify inappropriate use of internet i.e. that is contrary to P60/06 (and G0802). Will involve monthly audit of access to a predetermined list of likely inappropriate websites such as E-Bay, Facebook etc.	Monthly commencing January 2011	Audit & Inspection
Driver Validation Scheme (DVS)	DVS is an information system provided by the DVLA which is of considerable operational benefit, primarily with Roads Policing. The terms of access (contained in a Code of Connection) require that Essex Police carry out dip sampling on a monthly basis.	Monthly commencing November 2010	Information Security
Data Quality	A data quality profile and cleansing tool is currently being procured. Once in place its functionality and resource levels will help determine its application. It is anticipated that attention will focus on some Person Standards within CrimeFile, Intelligence & PROtect.	Daily commencing January 2011 (subject to change)	Data Quality and Compliance
Information Security Breaches	As per G0804 Information Security will oversee the handling of information security breaches.	Ad hoc	Information Security
Transaction Validations	Transaction Monitoring in accordance with P46/07. Subject to resource levels this will commence with PNC, followed incrementally by Intelligence, PND and CrimeFile (order of last three to be determined by the IMB at a later date).	Daily commencing January 2011	Audit and Inspection
Crime Recording & Incident Recording and Finalisation	Compliance testing against the Home Office Counting Rules and the National Crime Recording Standards. Ad Hoc audits will be undertaken following the emergence of reputational risk	Monthly	Audit and Inspection

Crime Recording and Finalisation	Compliance testing against the Home Office Counting Rules and the National Crime Recording Standards.	Daily	Crime Statistics
PNC Wanted Audit	This is designed to test whether persons listed as Wanted on PNC, and therefore subject to arrest, have been appropriately marked as such. In addition it may be possible to identify wanted persons who had not been marked as such on the PNC when they should have been. Data is entered onto or removed from the PNC by the PNC Bureau in response to notifications from divisions via Wanted 1 forms or from the SWARM (Warrants) database. The audit could be extended to include Missing Persons along similar lines – their details should be on the Compact database too, or further still to Locate Traces and Orders should resources allow.	Quarterly	Audit & Inspection
PNC Vehicles – Lost/Stolen	This is designed to test whether vehicles listed as Lost/Stolen on the PNC, and therefore subject to arrest, have been appropriately marked as such. Data is entered onto or removed from the PNC by the PNC Bureau. The audit could be extended to include Act Reports – these are 'higher' level information reports that feed into ANPR and therefore can affect the deployment of ANPR teams.	Quarterly	Audit & Inspection
Ad Hoc	Subject to a risk-based approach additional work may be prioritised. This is only likely to occur where the risk is significant and pressing, and will inevitably result other work being displaced, such is the pressure in these two areas.	Ad Hoc	Information Management Audit & Inspection

3 Recommendations

3.1 The IMB is asked to

3.1.1 endorse the programme of work described above;

3.1.2 sanction revisions to the above to be presented to the IMB as circumstances dictate;

3.1.3 agree that summaries or management reports are presented by those conducting the above as required by the Chief Information Officer in their role as Chair of the IMB.