June 2017

Annual Report of the Senior Information Risk Owner (SIRO)

Amanda Cooper, Chief Information Officer
Hampshire Constabulary and Thames Valley Police

Executive summary

This report provides a summary of Information Assurance (IA) and Information Governance (IG) activity across Hampshire Constabulary and Thames Valley Police during 2016-17 in order to provide assurance that information risks are being managed effectively.

The report also provides an update on the following:

- achievements relating to IA and IG for the period 1 April 2016 to 31 March 2017
- the Forces' compliance with legislative and regulatory requirements relating to the handling of information, including compliance with the Data Protection Act (1998) and Freedom of Information Act (2000),
- data loss incidents during 2016-17 and a summary of other incidents relating to any losses of personal data or breaches of confidentiality, and
- the planned direction of IA and IG activity during 2017/18 to support the strategic objectives of Hampshire Constabulary and Thames Valley Police.

1. Introduction

1. Hampshire Constabulary and Thames Valley Police have a duty to obtain and use a wide variety of information in order to discharge their duties effectively and to keep people safe. The information is an asset to be valued, protected and exploited but can also become a liability if it is inappropriately recorded, interpreted or disclosed.

2. The legacy of Soham, increasing cross-border and cross-disciplinary working, and the digital policing agenda require information to be more accessible, linked and reused. Increasingly however, there is a growing expectation from the Government, the Information Commissioner, the media and the general public that the security used to protect information should consistently meet high standards - and that data held should be proportionate, and only accessed and shared when necessary. The introduction of the EU General Data Protection Regulation next year will only heighten these expectations.

3. Structures and processes are in place to manage risks to the Forces' information. The Joint Information Management Unit (JIMU), hosted by Thames Valley Police, came into existence on 1 April 2012 to provide Information Governance (IG) and Information Assurance (IA) support to both forces under the collaboration arrangements. The more technical aspects of IA were transferred to the joint ICT department in October 2015 to ensure that new processes and structures being designed for the ICT transformation were fit for purpose, and that appropriate system design and risk mitigation was put in place to deal with increasing cyber threats. The two teams continue to work together closely to manage information risks, and the new processes reflect this. These departments are required to operate under both guidance and mandate from the NPCC, the Home Office and Cabinet Office (CESG).

4. The purpose of this report is provide assurance that information risks are being managed effectively and provide an update on the following:

   - achievements relating to IA and IG for the period 1 April 2016 to 31 March 2017
   - the Forces' compliance with legislative and regulatory requirements relating to the handling of information, including compliance with the Data Protection Act (1998) and Freedom of Information Act (2000),
   - any serious data loss incidents during 2016-17 and a summary of other incidents relating to any losses of personal data or breaches of confidentiality, and
   - the planned direction of IA and IG activity during 2017/18 to support the strategic objectives of Hampshire Constabulary and Thames Valley Police.

2. Structure and governance

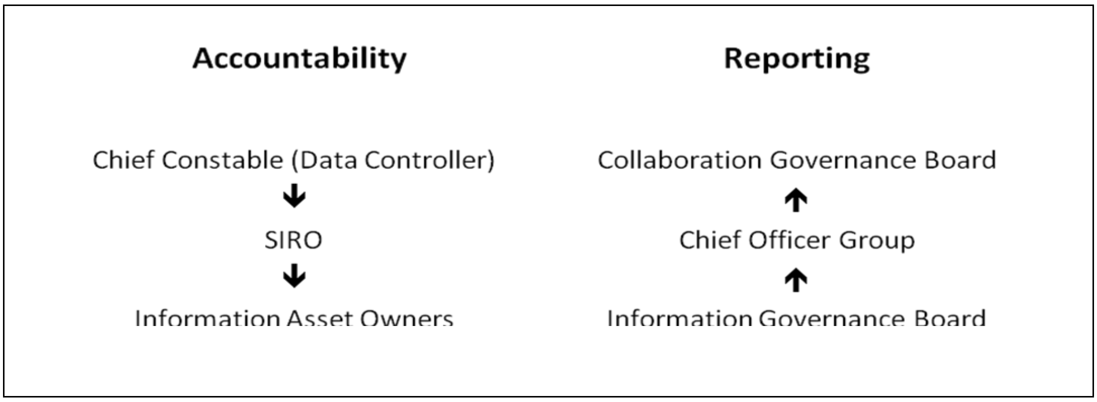
5. The Heads of ICT and JIMU both report to the Chief Information Officer (CIO). The CIO also fills the role of Senior Information Risk Owner (SIRO) for the two forces, making strategic decisions in regard to information risks, particularly when there is a potential conflict between operational and information security requirements.

6. Support for the SIRO is provided within the organisational structure by:

- Head of Information Communications & Technology
- Head of Information Management
- Senior Information Governance Manager
- Senior Public Access Manager
- Senor Records Manager
- Information Security Manager.

7. In addition, senior business leaders have been appointed as Information Asset Owners (IAOs) to provide governance and oversight for significant collections of information. They are responsible for ensuring this information is managed in accordance with policy and for identifying and mitigating any associated risks.

8. The joint Information Governance Board, which is chaired by the CIO, is responsible for monitoring the effectiveness of policy, procedure, training and guidance in regard to Information Governance, and identifying information risks. Critical risks are recorded on the Strategic Risk Register, and where appropriate, escalated to the Chief Officer Group and the Collaboration Governance Board.


Accountability
Reporting
Chief Constable (Data Controller)
SIRO
Information Asset Owners
Collaboration Governance Board
Chief Officer Group
Information Governance Board

9. Please see *Appendix A* for national governance arrangements.

3. Information Governance and Information Assurance Delivery 2016-17

3.1 Regional collaboration

10. A Regional Security Manager role was introduced in November 2016 to lead the harmonisation of Information Assurance (IA) polices, processes and working practices across the four South East Police forces. To support this, a Regional IA Board (RIAB) has been established, reporting to the South East Regional IT Board (SERIT) with membership from across the four forces and representation from the National Police Information Risk Management Team (see *Appendix B*).

11. The RIAB has had three successful meetings and has already started working on regional IA initiatives such as cloud security principles and smartphone application governance.

12. The Head of Information Management has also set up a regional Information Management Forum (see Appendix C) to share knowledge and good practice, align information governance policies and enable a co-ordinated approach to responding to legislative and national policy requirements.

3.2 Improvements to Information Assurance processes

13. The following improvements have been implemented:

- Terms of reference for IA to ensure consistency and focus within the team and clarity for the business when engaging with IA;
- A more business focused risk assessment process to provide a pragmatic and proportionate approach to local and regional projects, with working groups established for Contact Management, Enterprise Resource Planning (ERP) and secure data / cloud storage;
- A project lifecycle approach which clearly shows the engagement model between the business, IA and ICT Business Relationship Managers;
- A review of key information security policies to ensure that risks are appropriately managed without unnecessarily restricting operational needs, with the aim of alignment across the South East region;
- An increase in IA resource through successfully filling the permanent IA advisor role;
- Regular knowledge sharing across IA, IT Security and the Joint Information Management Unit.

3.3 Rollout of Government Security Classification Policy (GSCP)

14. Both Forces successfully migrated from the Government Protective Marking Scheme (GPMS) to the Government Security Classification (GSC) policy on 1 October 2016. A bilateral project was led by JIMU, in liaison with Sussex and Surrey to ensure a consistent regional approach.

3.4 Information Asset Ownership

15. Each Information Asset Owner has been specifically consulted and briefed on their responsibilities and accountability, and has identified Data Guardians to support them in their role.

16. The Information Asset Register has been updated to identify each information asset, the asset owner, data guardian and risk management plans. Risks that are beyond local treatment are escalated by the JIMU to the strategic information governance board. Communication and sharing of good practice is facilitated through a dedicated Yammer group and a newsletter.

17. In recognition of this work, JIMU has been shortlisted in the Strategic category for a 2017 Risk Awards administered by Alarm, an organisation for risk professionals working in the public sector.

3.5 Public Services Network (PSN) Compliance

18. Having successfully met the requirements to migrate from the CJX to the Public Services Network (PSN) during 2015-16, it was disappointing that both forces did not gain approval for renewal of their PSN Accreditation this year following a transfer of the approval process to Government Digital Services (GDS).

19. GDS have provided feedback detailing the reasons for noncompliance which were largely related to technical vulnerabilities within the legacy IT systems and infrastructure which it was not feasible to fully address before the time of PSN renewal, e.g. Altaris, which is due to be replaced by the Contact Management Platform later this year.

20. Without being complacent, it should also be noted that a significant number of other forces were also unsuccessful in obtaining reaccreditation, including Surrey and Sussex Police.

21. The lack of accreditation does not affect existing PSN connections but means that the forces are unable to purchase additional PSN connectivity for projects such as secure data / cloud storage until GDS provide an approval certificate. However, the potential impact of this on strategic projects is currently low: it estimated that the remedial work to obtain accreditation will be completed by December 2017 and the existing PSN connections can be used as an interim solution.

22. Mitigation to manage any interim cyber risk to the forces has been put in place through the review of complementary controls such as security of the IT network perimeter, antivirus software and the ability to respond to a cyber-attack.

3.6 Requests for information

23. During 2016-17, a total of 704 Subject Access Requests were made to Hampshire Constabulary under the Data Protection Act, and 729 to Thames Valley. The legal deadline for the Force to respond is 40 working days. This was met in 96.4% and

98.4% of cases respectively (compared with 749 requests / 99.1% compliance and 798 requests / 98.4% compliance respectively in 2015-16).

24. During 2016-17, a total of 1,379 requests were made under the Freedom of Information (FoI) Act to Hampshire Constabulary and 1,462 to Thames Valley. The legal response deadline is 20 working days and this was met in 96.4% and 99.4% of cases respectively (compared to 1,412 requests / 97.9% compliance and 1,487 requests / 98.6% compliance respectively in 2015-16).

25. More detailed statistics are available in *Appendix D*.

26. During this period, the Information Commissioner's Office issued two decision notices to Hampshire Constabulary regarding complaints in the way that FoI requests had been handled. One complaint was upheld, the other was not. Both cases are currently being appealed through the Information Tribunal. One decision notice was issued to Thames Valley Police during the same period and the complaint was not upheld.

3.7 Information Sharing Agreements

27. In order to enable information sharing with partners whilst still remaining compliant with the Data Protection Act and the Code of Practice on the Management of Police Information (MoPI), JIMU provides support to the Forces in ensuring that appropriate Information Sharing Agreements (ISAs) clearly set out what information can be shared and how it should be managed. These cover a wide range of areas, including support for Multi Agency Sharing Hubs (MASH), mental health issues, emergency accommodation for homeless people, and various 'watch' schemes, e.g. Pubwatch.

28. At the end of March 2017, there were 96 ISAs in place in Hampshire and 86 in Thames Valley. Copies of the ISAs are available at:

- https://www.hampshire.police.uk/about-us/publications-and-documents/information-sharing-agreements/
- https://www.thamesvalley.police.uk/search/?q=information+sharing.

3.8 Protective Monitoring

29. A managed service from Qinetiq has been procured to provide protective monitoring for the two forces. Forty high-risk devices and servers will be continuously monitored for unusual activity with potential issues escalated to the ICT Service Desk for investigation and resolution if necessary. It is anticipated that real-time detection and intervention of potential issues will minimize the impact of malicious attacks.

4. Information Security Incident Management

4.1 Summary of reported security incidents 2016-17

30. A total of 351 information security incidents were reported during 2016-17 (65 in Hampshire and 286 in Thames Valley). A summary can be found at *Appendix E*.

31. No incidents met the threshold for reporting to the Information Commissioners' Office during 2016-17.

4.2 Virus/malware detected 2016-17

32. A total of 1,620 attempts to infect the Hampshire IT infrastructure were prevented by the Sophos system during 2016-17, with a similar 1,619 attempts in Thames Valley. More information is available at *Appendix F.*

5. SIRO decisions 2016-17

The following decisions were escalated to the SIRO during 2016/17:

Date of Decision	Subject	Description	Force
21/06/2016	Niche RMS	Use of real personal and operational data to test the design and capability of the Contact Management Platform.	Both
21/07/2016	IL4 Terminals at Reading PS	Omit the use on PIN locks on an office environment where IL4 terminals are used on an ad hoc basis.	TVP
21/07/2016	Screen time out in Contact Management	Removal of screen time out in specific Contact Management locations	Both
25/08/2016	Digitisation of Microfiche Collection	Outsourcing of digitisation work to a third party	TVP
21/09/2016	Winchester PHQ Outage	Request to allow temporary domain account sharing by Force Enquiry Centre (FEC) staff members.	Hants
22/09/2016	Yammer	Access to Yammer from non-Force owned devices	Both
05/10/2016	Speech and Text	Installation of Speech and Text analytics software on development environment to be completed remotely by United States based engineers	Both
21/02/2017	Use of Azure for CMP	Use of Microsoft Azure Cloud for hosting the Contact Management Platform	Both

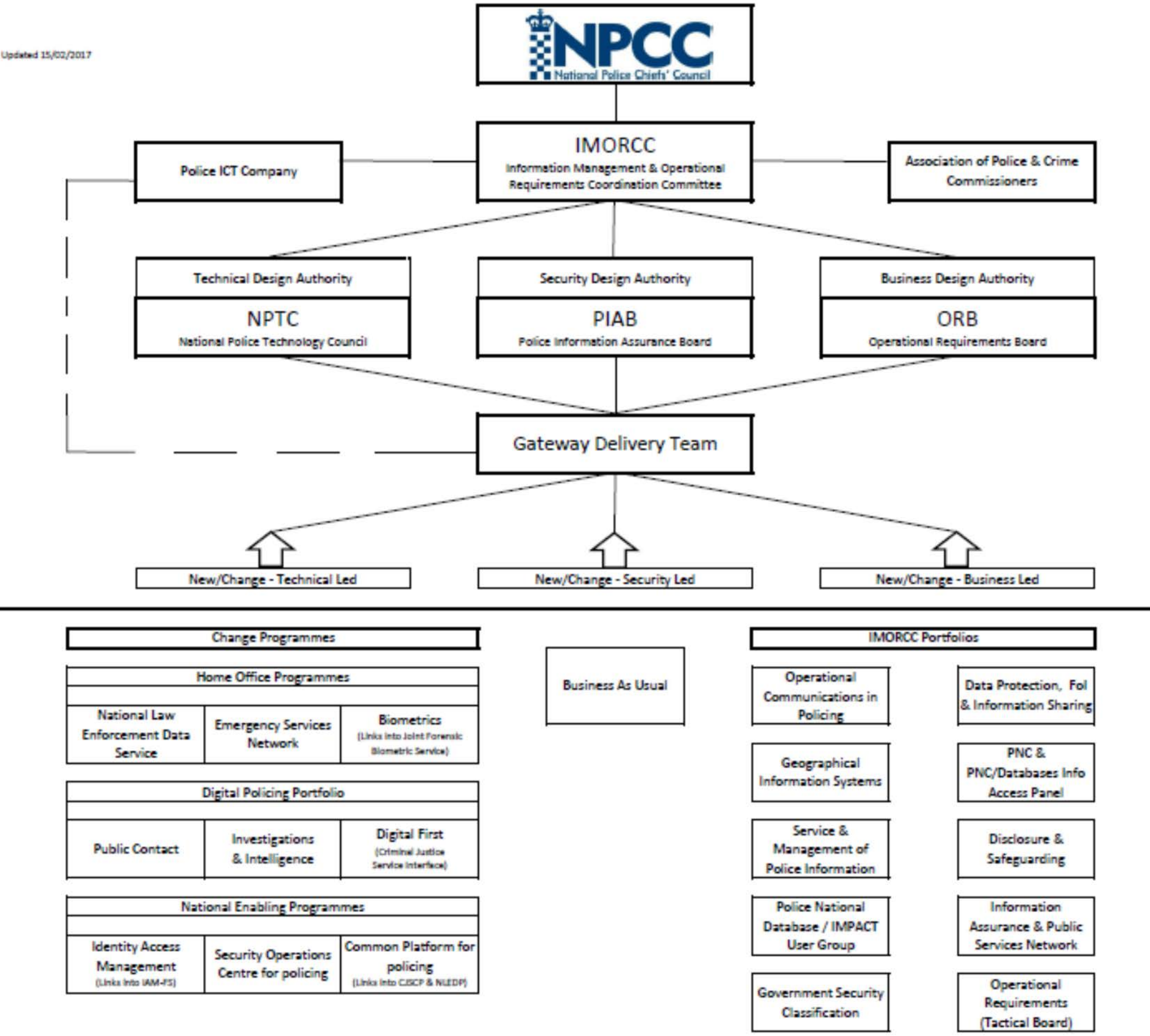
6. Planning for 2017/18

33. Key areas of focus will be:

- Continue to review and update of security policies/procedures and working practices to provide a consistent approach across the Forces, aligned with the regional approach;
- Continue to support the Information Asset Owners in carrying out regular risk assessments and compile and analyse common risk areas;
- Prepare the two Forces for the introduction of the EU General Data Protection Regulation (GDPR);
- Adopt a standards based approach for IA through adoption of the ISO/IEC 27001 framework;
- Test the regional capability to respond to a cyber-attack through simulated cyber-attack exercises;

- Improve IA engagement with the business to change it from being perceived as a barrier to being seen as a business enabler through:
  - Adoption of a pragmatic and proportionate risk assessment methodology;
  - Definition of the roles and responsibilities of IA though development of a Responsible / Accountable / Consult / Inform (RACI) model;
  - Improved communication to the business on how and when to engage with IA;
  - Encouraging the business to challenge decisions made by IA to ensure they are proportionate and justified;
- Conduct an IT Health Check of the Hampshire / TVP IT environment for submission to GDS for PSN compliance;
- Implement an in-house vulnerability scanning capability to allow the forces to conduct quarterly tests to verify that remediation activity following the annual IT Health Checks has been successful and to identify any new vulnerabilities;
- ‘Go live’ of the protective monitoring service.

Appendix A - National governance model


Updated 15/02/2017
NPCC
National Police Chiefs' Council
Police ICT Company
IMORCC
Information Management & Operational Requirements Coordination Committee
Association of Police & Crime Commissioners
Technical Design Authority
NPTC
National Police Technology Council
Security Design Authority
PIAB
Police Information Assurance Board
Business Design Authority
ORB
Operational Requirements Board
Gateway Delivery Team
New/Change - Technical Led
New/Change - Security Led
New/Change - Business Led
Business As Usual

Change Programmes

Home Office Programmes		
National Law Enforcement Data Service	Emergency Services Network	Biometrics (Links into Joint Forensic Biometric Service)

Digital Policing Portfolio		
Public Contact	Investigations & Intelligence	Digital First (Criminal Justice Service Interface)

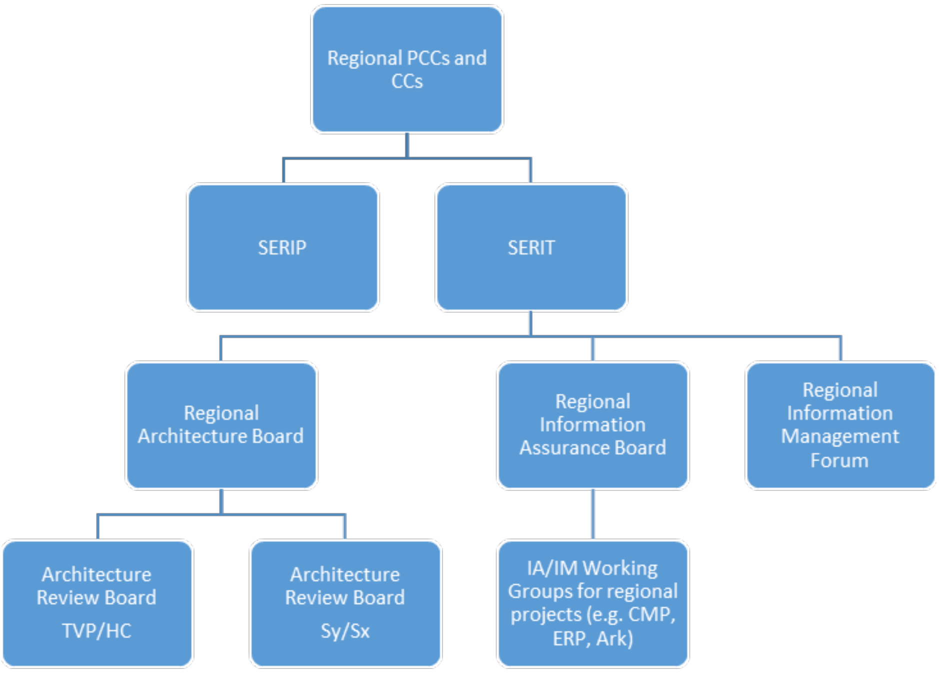
National Enabling Programmes		
Identity Access Management (Links into IAM-FS)	Security Operations Centre for policing	Common Platform for policing (Links into CJSCP & NLEDP)

IMORCC Portfolios

Operational Communications in Policing	Data Protection, FoI & Information Sharing
Geographical Information Systems	PNC & PNC/Databases Info Access Panel
Service & Management of Police Information	Disclosure & Safeguarding
Police National Database / IMPACT User Group	Information Assurance & Public Services Network
Government Security Classification	Operational Requirements (Tactical Board)

Appendix B – Governance for Regional Information Assurance

The following governance structure for the region has been proposed to promote collaboration:


Regional PCCs and CCs
SERIP
SERIT
Regional Architecture Board
Regional Information Assurance Board
Regional Information Management Forum
Architecture Review Board TVP/HC
Architecture Review Board Sy/Sx
IA/IM Working Groups for regional projects (e.g. CMP, ERP, Ark)

The aim of the Regional Information Assurance Board (RIAB) is to provide strategic leadership for the establishment of:

a) Common practices and standards for the security and management of information and assets held by the South East Regional IT (SERIT) partner forces, and

b) A risk based approach to security and information assurance (IA) in line with legislation, and current industry and Government standards.

The RIAB is responsible for:

- Defining an IA vision which supports the strategic goals of the four force collaboration and creates a culture of responsible and compliant data exploitation and sharing
- The definition, publication and ongoing maintenance of regional IA principles and standards which support and align with the national strategic direction for IA and security
- Harmonisation of IA processes, policies and working practices across the region to ensure a consistent and transferable approach to IA

- Validation of regional system designs and technology change programmes against those principles and standards; adopting a risk-driven approach as appropriate to the support operational requirements and public safety
- The development, support and regular review of the IA roadmaps for the region reflecting the short, medium and long term vision
- Providing direction and support to the SERIT Board on the use of new information and communications technology (ICT) and data sharing without compromising the Region’s information security
- Championing more pragmatic and proportionate use and exploitation of IA to support operational and business requirements
- Sharing good practice and lessons learned, and encouraging innovative thinking to support the identification and implementation of effective solutions for IA
- Providing an interface between local Force IA and the SERIT Board, ensuring information risk is clearly articulated and understood at senior level
- Working cooperatively with the Regional Architecture Board and the Regional Information Management Forum (and other regional groups as applicable) to ensure a holistic and consistent approach to secure design, data governance and IA

Appendix C - Regional Information Management Forum

Terms of Reference

Purpose

The Information Management Forum will provide the necessary governance structure to:

- champion more effective use and exploitation of information to support operational and business requirements.
- enable compliance with local, regional, national and legislative requirements for information management
- support consistency and convergence of information management working practices across the region
- share good practice and lessons learned, and encourage innovative thinking to support the identification and implementation of effective solutions for information management
- provide an interface between local information management boards and South East Regional IT (SERIT) board.

Membership

Core members:

- Head of Information Management, Hampshire & Thames Valley
- Force Information Management Programme Manager, Sussex
- Head of Service Quality, Surrey

Core members will be expected to carry appropriate authority for decision making and subsequent activity within home forces, subject to the governance processes within their force.

Core members may bring along other team members as appropriate.

Core members are expected to provide a deputy when they are unavailable to attend. Other attendees by invitation.

Governance

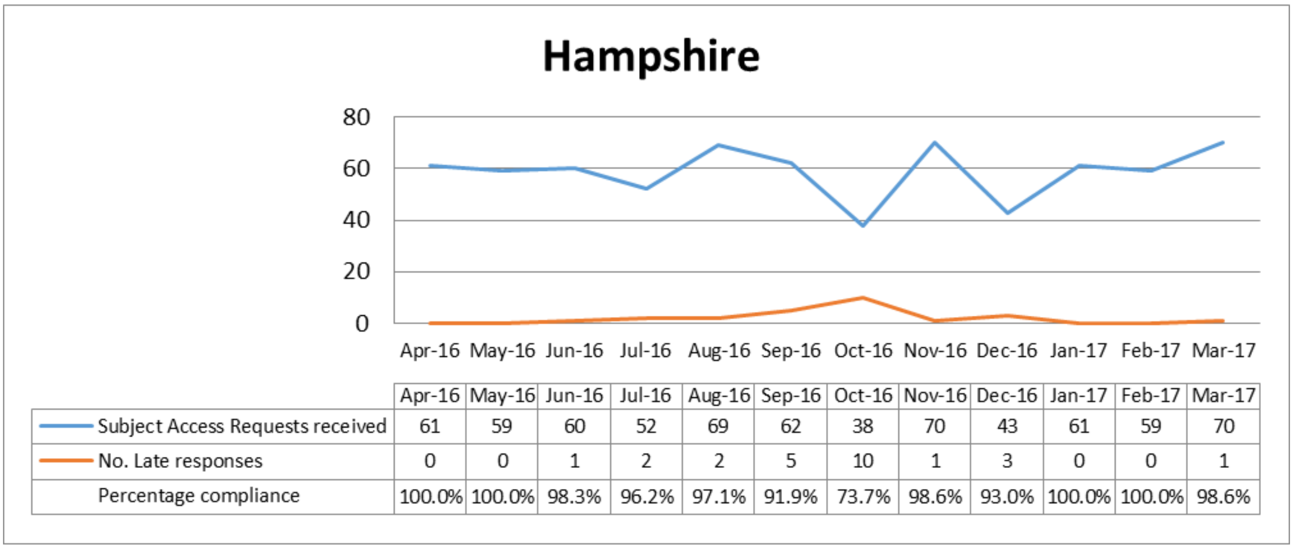
Meetings will be held monthly. Any issues that require attention between meetings will be dealt with via email/teleconference or an extraordinary meeting if appropriate.

It is envisaged that forces will escalate local issues to the regional forum and up to SERIT if appropriate.

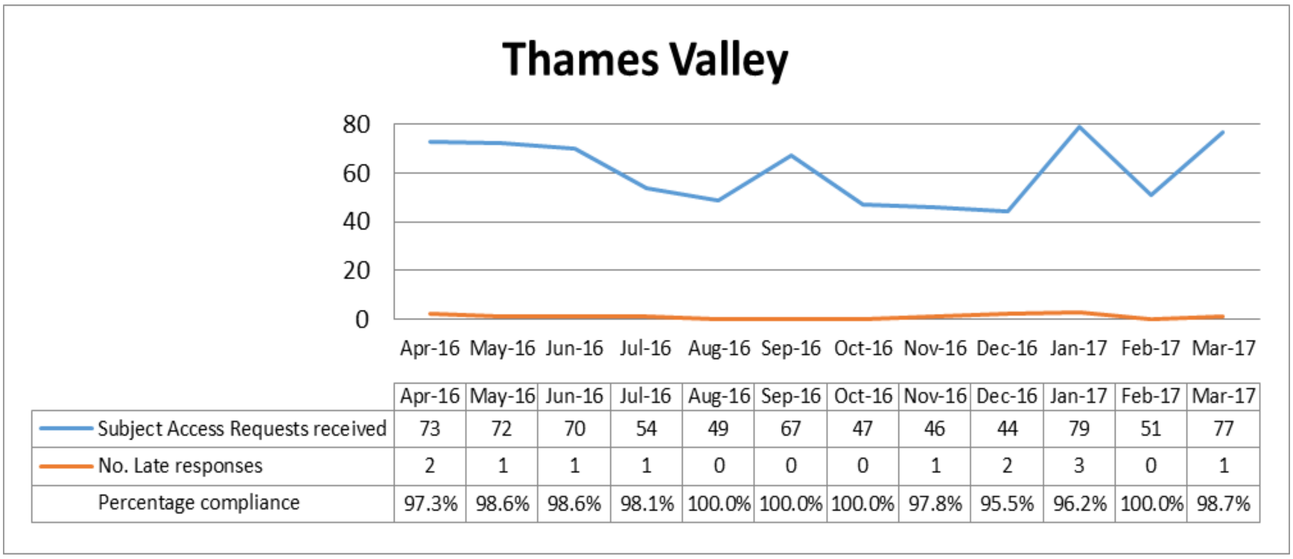
The chair will rotate every three months. The chair’s responsibility includes arranging the agenda, maintaining a Risks / Actions / Issues / Decisions (RAID) log, and producing a quarterly highlight report for SERIT.

Appendix D – Legislative compliance regarding requests for information

Subject Access requests 2016-17 (response deadline 40 working days)

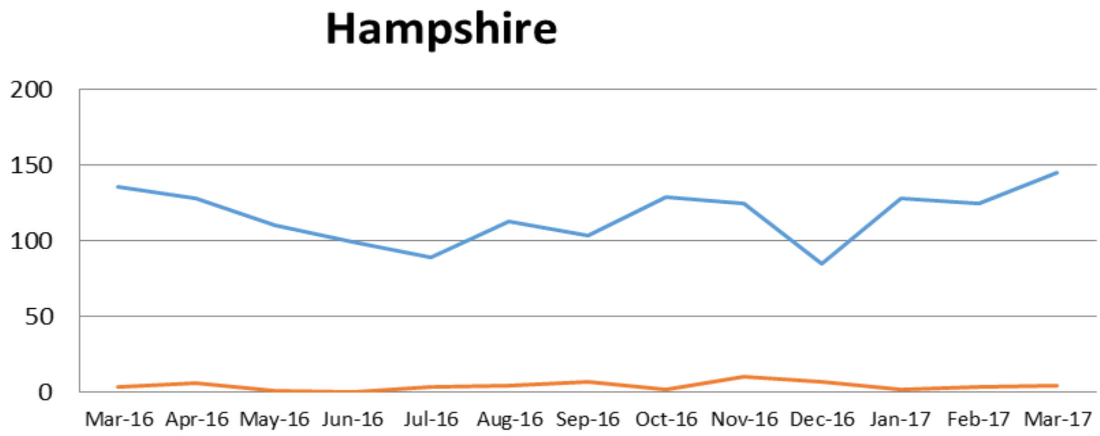


	Apr-16	May-16	Jun-16	Jul-16	Aug-16	Sep-16	Oct-16	Nov-16	Dec-16	Jan-17	Feb-17	Mar-17
Subject Access Requests received	61	59	60	52	69	62	38	70	43	61	59	70
No. Late responses	0	0	1	2	2	5	10	1	3	0	0	1
Percentage compliance	100.0%	100.0%	98.3%	96.2%	97.1%	91.9%	73.7%	98.6%	93.0%	100.0%	100.0%	98.6%

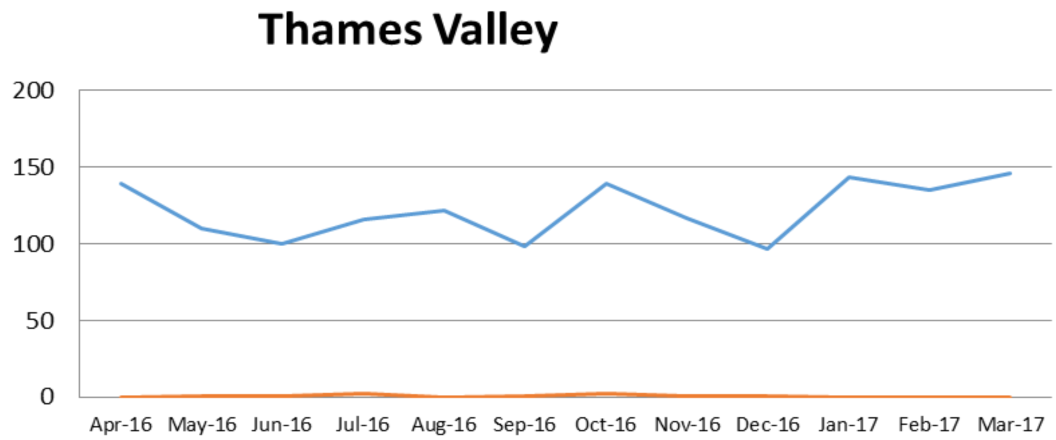


	Apr-16	May-16	Jun-16	Jul-16	Aug-16	Sep-16	Oct-16	Nov-16	Dec-16	Jan-17	Feb-17	Mar-17
Subject Access Requests received	73	72	70	54	49	67	47	46	44	79	51	77
No. Late responses	2	1	1	1	0	0	0	1	2	3	0	1
Percentage compliance	97.3%	98.6%	98.6%	98.1%	100.0%	100.0%	100.0%	97.8%	95.5%	96.2%	100.0%	98.7%

Freedom of Information requests 2015-16 (response deadline 20 working days)



	Mar-16	Apr-16	May-16	Jun-16	Jul-16	Aug-16	Sep-16	Oct-16	Nov-16	Dec-16	Jan-17	Feb-17	Mar-17
FoI Requests received	136	128	110	99	89	113	103	129	125	85	128	125	145
No. Late responses	3	6	1	0	3	4	7	2	10	7	2	3	4
Percentage compliance	97.8%	95.3%	99.1%	100.0%	96.6%	96.5%	93.2%	98.4%	92.0%	91.8%	98.4%	97.6%	97.2%



	Apr-16	May-16	Jun-16	Jul-16	Aug-16	Sep-16	Oct-16	Nov-16	Dec-16	Jan-17	Feb-17	Mar-17
FoI Requests received	139	110	100	116	122	98	139	117	97	143	135	146
No. Late responses	0	1	1	2	0	1	2	1	1	0	0	0
Percentage compliance	100.0%	99.1%	99.0%	98.3%	100.0%	99.0%	98.6%	99.1%	99.0%	100.0%	100.0%	100.0%

Appendix E - Summary of reported security incidents 2016-17

Incident Type	**Hants**	**TVP**
E-mail misuse	1	9
Unplanned outage	0	1
Unauthorised disclosure	14	16
System misuse	4	0
Account sharing	1	0
Loss or theft of technology assets	41	179
Paper documents	4	27
Crypto	0	0
Data storage issues	0	4
Removable media issues	0	0
Unauthorised equipment	0	1
Unauthorised software	0	1
Malicious software	0	2
Insecure disposal of media or documents	0	2
Airwave	0	44
Unauthorised access to systems/data	0	0
Totals*	**65**	**286**

* A joint online solution using vFire is being implemented which will streamline incident reporting across both forces and should address suspected current under-reporting in Hampshire.

Appendix F - Virus/malware attempts detected 2016-17

Most common viruses / malware detected

	Hampshire	Thames Valley
Mal/AutoInf-B	9	148
Mal/DrodZp-A	489	106
Mal/Generic-S	216	89
Mal/Phish-A	114	33
Mal/Zbot-DY	152	5
Troj/Agent-APQR	110	15
Troj/DocDl-WI	1	616
Troj/JSAgent-GM	56	0
Troj/JSRedir-RX	43	35
Troj/PDFUri-AH	69	0
Troj/ZipMal-GT	103	0
W32/Patched-I	54	7