Document Name	National Approach to Information Assurance 2014 - 2017
File Name	National Approach to Information Assurance v1.doc
Author	David Critchley, Dave Jamieson

Authorisation	PIAB and IMBA
Signed version held by	National Police Information Risk Management Team

For additional copies, or to enquire about the content of the document, please contact the National Police Information Risk Management Team at or information.assurance@homeoffice.pnn.police.uk

Table of Contents

Deleted: 9

Deleted: 10

Deleted: 11

Deleted: 12

Deleted: 13

Deleted: 14

1. Purpose.

1.1. The purpose of this national approach is to set out a three year strategic direction for further developing Information Assurance (IA) capability and effectively embedding an IA culture across the Police Service.

1.2. This paper replaces the 2010 -2013 Police Service IA Strategy.

1.3. It provides information on the requirements placed on the Police Service under the Community Security Policy (CSP), such as compliance with the Security Policy Framework, the Community Code of Connection, the HMG IA Maturity Model and Assessment Framework and the Modular Risk Management Accreditation Document Sets for police systems.

1.4. Annex A shows the relationship between the UK Cyber Security Strategy, the Community Security Policy and the 'Aims' on this National Approach to IA.

2. Scope

2.1. This national approach is owned by PIAB and has been approved by the Chief Constables Council and applies to members of the Police Service community[1].

3. Introduction.

3.1. Policing is an increasingly information-led activity. In order that all Forces, their Police and Crime Commissioners, organisations working in policing, their partners and the public can have confidence in the integrity and availability of policing information and its secure storage, processing and disposal, it is necessary to have robust IA structures and processes in place. Without these there is a significant and realisable risk of compromise potentially leading to the facilitation of crime, public safety issues, hindrance to investigations, financial loss, damage to organisational reputation and consequently a reduction in confidence from partners and the public [2].

3.2. The national approach to IA reflects the increasing value of information to the Police Service, and it is increasingly used and shared in policing and with partner organisations. The intention is for IA to enable police operations and police improvement initiatives. The way that information systems are evolving in the Police Service increases the requirement for Information Risk Management (IRM) and governance, across their delivery, management, use and secure disposal. There needs to be an emphasis on consistency, transparency and ownership of IA processes, and on measured improvement of those processes.

3.3. For clarity, the HMG definition of Information Assurance is;

[1] The national approach to IA does not apply directly to delivery partners and suppliers of the police service, however through IAMM, IA requirements will be passed to them.

[2] Improvement in Public Confidence being a key theme of the National Improvement Strategy for Policing.

"Information Assurance (IA) is the confidence that information systems will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users."

4. Vision.

The vision for IA in the Police Service is articulated in the following statement;

An Information Assurance culture embedded across the police service enabling the effective use of police information in line with policing priorities.

5. Aims.

5.1. IA will be understood by all Police personnel and advice will be promoted and made available to all,

5.2. IA will be embedded in the culture of the Police Service at national and local levels, and aligned across Force/Agency boundaries.

5.3. Ownership and management of IA issues[3] will be clear to individuals, teams, partners and partnerships, enabling proper consultation with stakeholders prior to IA decisions.

5.4. Information Risk Management framework and processes will be clearly defined, so that individuals have a common understanding of assessment and treatment of risks, which would be conveyable between Forces, particularly in the area of Force collaboration and aggregated risk management.

5.5. IA standards and procedures continue to evolve; they must remain current and relevant to policing objectives and approaches.

6. Benefits

6.1. A number of benefits come out of implementing this national approach to IA:

6.1.1. Enhanced Public and Government confidence in the Police Service's ability to manage and handle information securely so that it is available when needed, trusted (of high integrity) and is only accessible to authorised users.

6.1.2. Greater trust and confidence when sharing information between organisations.

6.1.3. Delivery Partners, third parties and service providers are made aware of the need to secure police information.

6.1.4. Better protection from the risk of loss of availability, compromise of integrity or confidentiality of an organisation's data or information systems. Reducing the risk of reputational, financial penalties or legal liability.

[3] For IA Issues, read Risks, Threats, Vulnerabilities and security events

6.1.5. Enables organisations to be more aware of owned and shared information assets and different types of risks associated to those assets, providing:

- A deeper understanding of the business processes,
- Identify redundant or duplicated processes, which will reduce bureaucracy, and
- Improve performance and reduce operating costs.

6.1.6. Risk assessment will identify critical information assets, and the types of threat, vulnerability and risks to those assets. Enabling management to mitigate those risks through more cost effective targeted controls.

6.1.7. Reduce the number of security breaches and costs spent investigating them.

6.1.8. Reduce adverse publicity and enable the organisation to defend its integrity more effectively.

6.1.9. Provide a systematic approach and structure to enable continuous improvement.

6.1.10. Enhance the knowledge, awareness and importance of information risk management related issues at all levels within the organisation.

7. Objectives.

7.1. The overarching IA policy for the Police Service is embodied in the Community Security Policy. Therefore a key element of the national approach to IA is ensure the strategic aims of the CSP are implemented, these are:

7.1.1. Enable the delivery of policing by providing appropriate and consistent protection for the information assets of member organisations whether national, collaborative or local assets;

7.1.2. Comply with statutory requirements and meet the expectations of the Police Service to manage information securely;

7.1.3. Help assure Her Majesty's Government that Police Service elements of the Critical National Infrastructure (CNI) and Police Service connections to HMG networks and services are appropriately protected;

7.1.4. Facilitate effective participation with the National Security Strategy, Cyber Security Strategy and any future Government information strategies.

7.2. The relationship between the CSP, and the 'Aims' of the national approach to IA is shown in Annex A.

8. Initiatives.

8.1. The following strategic initiatives will be adopted by the Police Service in order to deliver the 'Aims' at section 5 above.

8.1.1. Ensure Chief Officer level commitment to IA.

8.1.1.1. The national approach to IA requires a strong, visible and sustained communicated, commitment to good IA from senior officers to all levels within Forces/Agencies.

8.1.1.2. Communications via the national governance structure that, includes Information Management Business Area (IMBA), National SIRO and Police Information Assurance Board (PIAB), are important in reinforcing this requirement.

8.1.2. Use of the Community Code of Connection, and Modular RMADS for National and Local Police information systems.

8.1.2.1. There is a national agreement that Forces/Ageencies who are signatories of the Community Security Policy complete the Community Code of Connection (CoCo).

8.1.2.2. It provides assurance to other signatories of the CSP that individual Forces/Agencies are securing police data and systems with a common, nationally agreed, level of protection commensurate with its sensitivity. The Community CoCo and Modular RMADS, encompasses CSP requirements not included in the IAMM.

8.1.2.3. Forces are required to review both annually and to submit the CoCo and supporting documents to NPIRMT[4]. Both document sets are to be subject to regular review and updates made available to the IA community across Forces/Agencies.

8.1.3. Wider use of the HMG Information Assurance Maturity Model (IAMM).

8.1.3.1. PIAB have determined that the CESG IAMM Assessment tool should be one of the key reporting mechanisms on Force/Agency compliance against the CSP and measuring IA maturity and improvement across the Police Service.

8.1.3.2. IAMM aligns the police service to Government departments and their agencies.

8.1.3.3. Engagement with IAMM assists Forces/Agencies in compliance with the Mandatory Requirements of the HMG SPF and IA Standards.

8.1.3.4. Forces/Agencies are required to submit reviews using IAMM by 31st May each year to the National Police Information Risk Management Team (NPIRMT)[4] acting for PIAB as part of the Protective Security and Risk Management Overview (PSRMO) process.

8.1.3.5. Forces/Agencies are expected to score at least 2[5] across Level 2 by 31 March 2014 and progress to score 2 across Level 3 (Established[6]) by March 2017.

8.1.3.6. Independent reviews may be conducted by NPIRMT[4]

[4] NPIRMT acts, in accordance with its mandate, on behalf of PIAB and the National SIRO.
[5] Score 2 is defined as "The majority of the Important evidence (High) and some of the Medium Importance (Medium) and Low Importance (Low) evidence is available and is satisfactory".
[6] Established is defined as "IA processes are institutionalised".

8.1.4. Enhancing Information Risk Management structures in forces and across the Police Service.

8.1.4.1. The police service has an increasingly communal approach to information and therefore there is an increasing degree of aggregated risk across Forces/Agencies. Risk decisions therefore require consultation of the appropriate risk owners.

8.1.4.2. Consistency across the police service in the way that information risk is assessed and treated will be facilitated by advice regarding implementation of standards, models (such as the National Police Information Threat Model) and tools for self-assessment against the Community CoCo (for national systems), and IAMM (for local implementation).

8.1.4.3. The standards and guidance must be clear, consistent and readily available. Information risk management frameworks must be aligned with that of corporate risk management frameworks.

8.1.5. Developing effective national and local incident management and recording across the Police Service.

8.1.5.1. Incident management will be matured within Forces/Agencies through IAMM (see 8.1.3 above).

8.1.5.2. The approach to reporting across the Police Service will be further developed to address incidents with impacts on the community, to encompass a wider range of incident reporting, prompt and proper investigation, and capture lessons learnt.

8.1.6. Improve IA Culture.

8.1.6.1. IA culture is the way that IA is regarded by individuals in the police. Forces/Agencies need to collaborate and exchange information with other government departments, agencies, and partners (such as forensic organisations, Crime and Disorder Reduction Partners, National Offender Management Service etc).

8.1.6.2. An element of trust is required in order to pass information to such delivery partners and 3rd parties, which is attained through proven IA measures, including information sharing agreements (ISAs) enforcing the Need to Know, personnel vetting policies, Protective Marking schemes and other procedural/technical controls for information exchange.

8.1.6.3. The IAMM provides a framework to assess the IA maturity of delivery partners. The IAMM controls are augmented with MOPI, NIM[7], and legislation such as the Data Protection Act.

8.1.6.4. Individuals need to recognise the relevance of IA to them and their own responsibilities. IA must be seen as an enabler rather than a restriction, and as an integral (and not isolated) aspect of police operations and information exploitation.

8.1.7. Enhance Information and Risk Management with delivery partners and third parties.

8.1.7.1. The Police risk management frameworks are developed to include the identification, communication and management of risks and

[7] National Intelligence Model (NIM)

risk treatments between Forces, Delivery Partners and 3rd parties, e.g. through the wider use of IAMM and other appropriate IRM tools across these entities.

8.1.8. Enhance IA within Local, Collaboration and National Programmes, Projects, Initiatives etc and also within 'live' services.

8.1.8.1. IA culture needs to be enhanced to encourage more accountability and ownership of IA risks by individuals, projects and programmes (such that improvements in policing that have any dependencies on IA, are considered at an early stage).

8.1.8.2. IA culture is enhanced and supported across live services by service management and suppliers.

8.1.9. Ensure policies and processes are clear and consistent, and readily accessible.

8.1.9.1. HMG IA standards, which are adopted by the Police Service as part of compliance with the Security Policy Framework, are augmented with police-specific standards and guidance (as appropriate).

8.1.9.2. The approach will ensure that best use can be made of developments in information technology without exposing the Police Service to unnecessary risk.

8.1.9.3. Where policies, processes and guidance do not address issues that are raised by programmes, the coverage of that guidance should be expanded to meet the demand.

8.1.9.4. These standards, guidance etc will be developed by NPIRMT and approved via PIAB and, if required, IMBA.

8.1.9.5. The standards will be clear and well communicated so that they are accessible and applied consistently.

8.1.10. IA capabilities will be defined and improved in support of the strategic initiatives described in this national approach to IA.

8.1.10.1. Some IA capabilities are made to the police service by NPIRMT, supporting a community approach to IA. Forces also need to develop and maintain their own IA capabilities to support their needs. Throughout the Police Service, the minimum roles to deliver the required IA capabilities need to be implemented within each Force/Agency.

8.1.10.2. IA capabilities across the Police Service will be consistent and in line with HMG/CESG guidance. The individuals who deliver these capabilities need to be appropriately trained, so they are comfortable and competent making IA decisions and executing their IA responsibilities in supporting business needs.

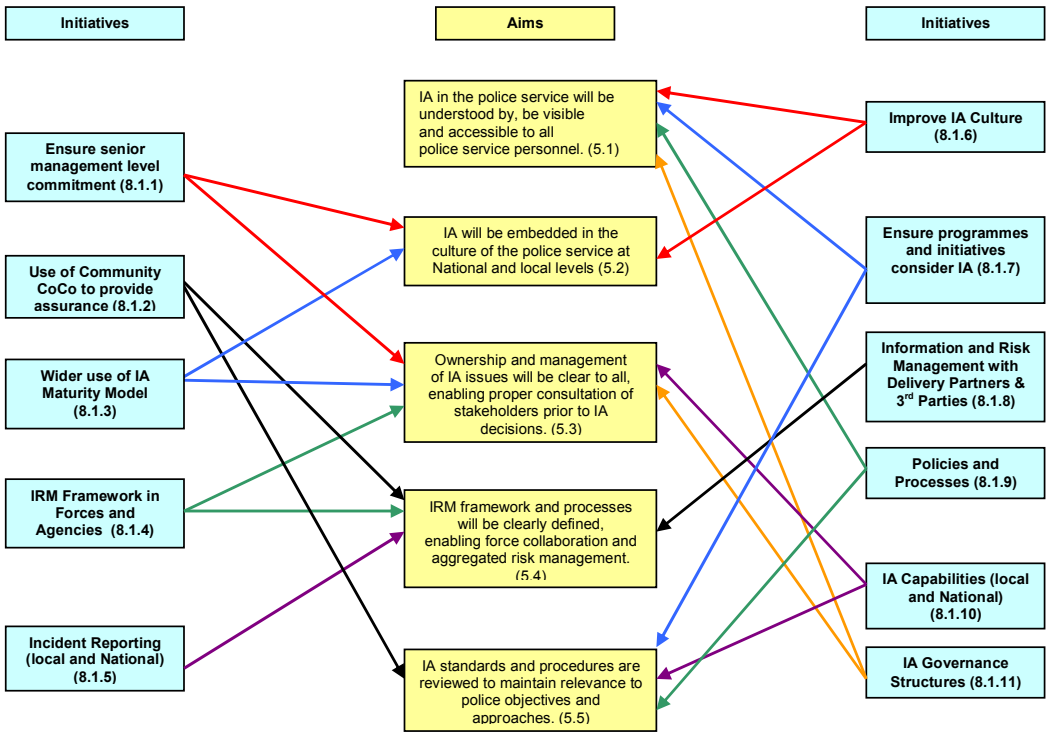
8.1.10.3. Professionalism in these roles is enhanced and optimised. The responsibilities associated with professional development for these roles should be included in terms and conditions. For further detail see Annex B.

8.1.11. Implementation of IA Governance Structures.

8.1.11.1. The Police Service comprises individual Forces and Agencies. The IA governance structure, including IA risk management and compliance, accountability, ownership and IA Services, must be identified and resourced within each entity to facilitate the 'Aims' of this National Approach to IA. The IA governance structure must have clear lines of communication and transparency.

8.1.11.2. The governance structure for IA must encompass Forces/Agencies, national systems; National Policing, government departments, delivery partners and 3rd parties (see also Annex C).

8.2. The following diagram shows how the 'Initiatives' in this national approach support the 'Aims' of this national approach to IA:



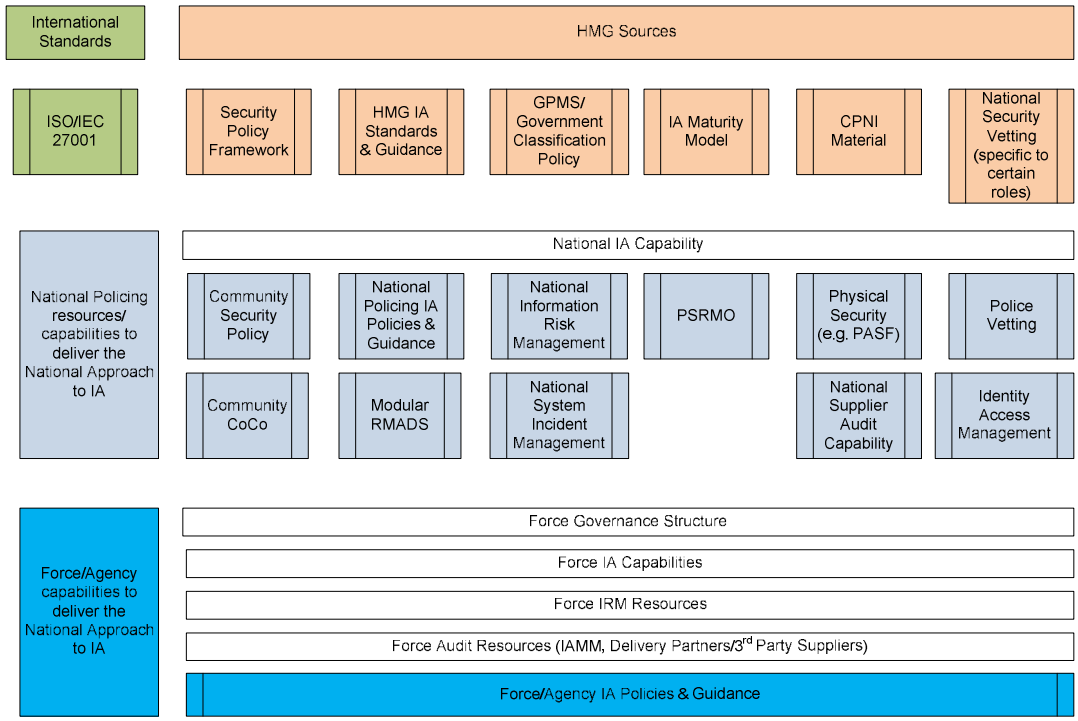
9. Governance of the National Approach to IA

9.1. The governance of this national approach rests with PIAB.

9.2. It is recommended that individual 'Aims' are allocated ownership, and plans are developed for the implementation of each. Progress against these plans should be reviewed on a regular basis (three monthly is suggested).

9.3. The collection and review of IAMM and CoCo returns by the NPIRMT will provide a comprehensive view of how the individual 'Aims' are being implemented at the Force level. Some aspects of the national approach to IA are implemented at the national level rather than within individual forces.

9.4. The various IA standards and policies that the Police Service have adopted/implemented; their placement within a national IA landscape and the relevant IA capabilities at a national and local level is illustrated in the diagram below:



10. Review Period.

10.1. The National Approach to IA will be subject to review on an annual basis due to the reliance of this strategy on supporting HMG policies, standards and National Policing requirements.

10. References.[8]

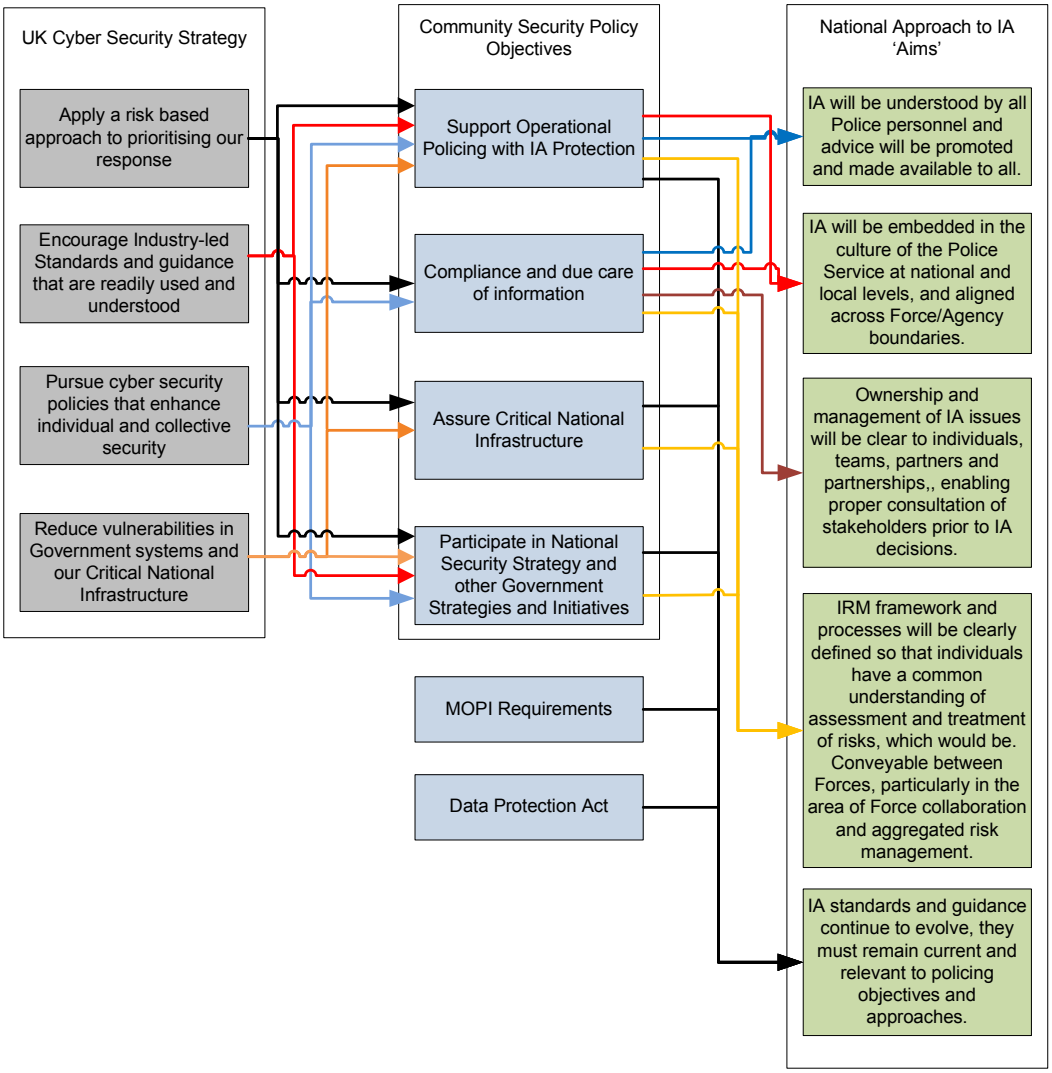
1. ACPO/ACPOS Community Security Policy (CSP) version 4 (March 2012)
2. HMG Security Policy Framework v11.0 (October 2013)
3. HMG Information Assurance Standard No 1&2: Risk Management and Accreditation of Information Systems, Issue 4.0 (April 2012)
4. HMG Information Assurance Maturity Model, v4.0 (May 2010)
5. Community Code of Connection, version 3.3 (25 April 2013)
6. National Policing Information Threat Model version 1.2 (November 2013)
7. Modular RMADS version 1.0 (April 2013)

[8] Version number refers to the version extant at the time of the publication of this Approach. The latest versions should always be referred to.

Annex A – Mapping Table

Traceability: Mapping of UK Cyber Security Strategy through the CSP to the national approach to IA

The diagram below illustrates how the UK Cyber Security Strategy is supported by the CSP strategic objectives which in turn are supported by the 'Aims' of the National Approach to IA.



Annex B - IA Capabilities

IA capabilities are the provision of advice or leadership to the Police Service, either by specific roles/teams using resources such as IT systems, toolkits and documentation where appropriate. IA capabilities can be provided at a **national** or **local** level.

Some IA capabilities are made available to the police service by NPIRMT. These capabilities support a community-based approach to IA, including:

- National Accreditor for the Police Service function;
- PolWARP, a forum for communication, reporting and discussion of threats, incidents and vulnerabilities;
- National policy and guidance development and maintenance function;
- Compliance and Audit function in relation to National Suppliers.

Other capabilities provide leadership in executing the national approach to IA, such as

- HMG IA Policy/Standards/Guidance;
- Police IA Policy/Standards/Guidance;
- IAMM guidance;
- CSP compliance advice;
- Guidance on the appropriate use and exploitation of IT.

However, it is not appropriate for all aspects of IA to be provided centrally. Forces need to develop their own IA capabilities to support their needs, in particular to embed the culture of information risk management. For example, guidance on the appropriate use and exploitation of IT will be provided locally as well as by NPIRMT for national services.

At a Force/Agency level, therefore, specific roles are responsible for advising staff on IA matters, and form a pivotal part of IA processes. As well as providing IA expertise they extend the capability to assess and manage risk.

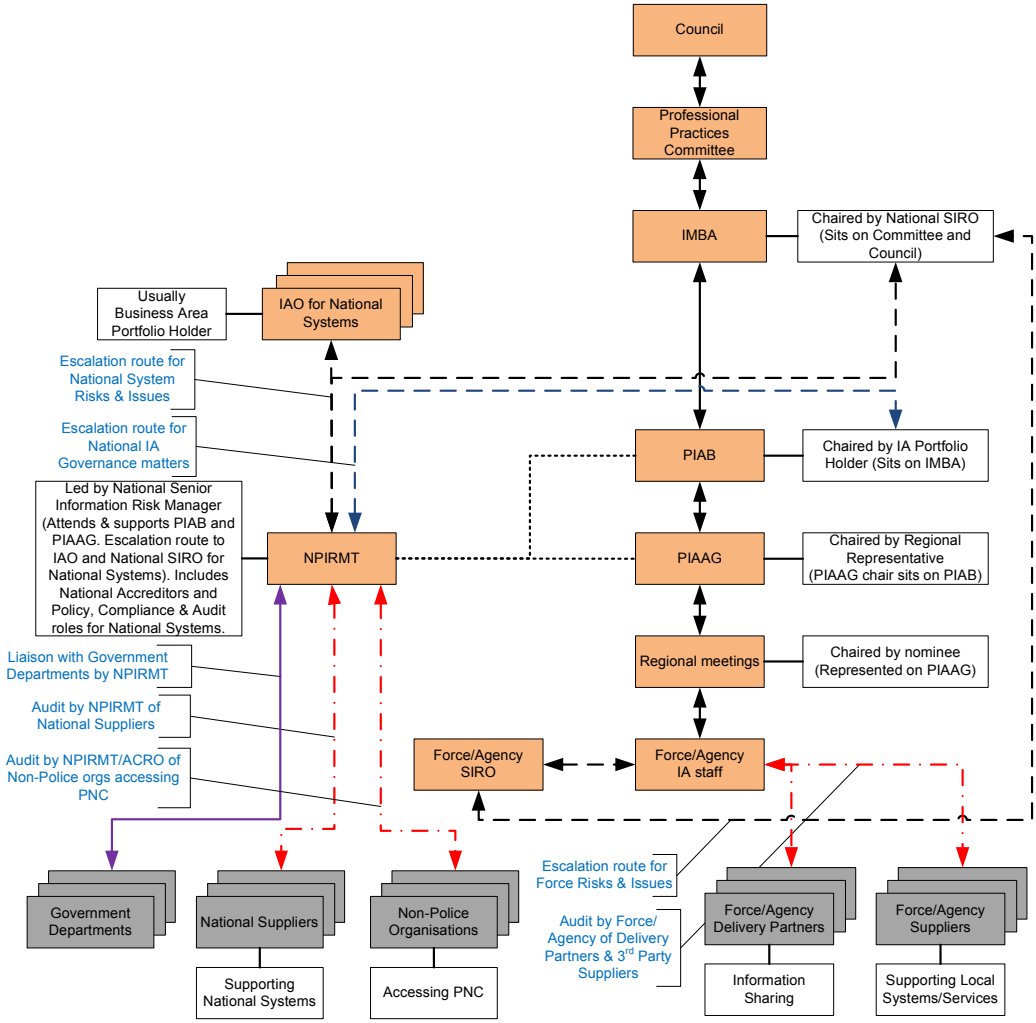
Throughout the Police Service, the minimum capabilities (e.g. SIRO, Accreditor, ITSO, ISO and IAO) to deliver the required IA capabilities need to be provided to each Force/Agency either at Force level or through collaboration. Consistency will be achieved through PIAG[9] and use of Cabinet Office and CESG guidance in developing the roles.

[9] Police Information Assurance Group

Annex C - IA Governance Structures

The governance structure for Information Assurance must encompass Forces/Agencies, national systems, National Policing, Delivery Partners, 3rd Party Suppliers and government departments.

The current Governance structure, showing the ownership of IA issues at Force and national levels, is shown below:



The above structure meets the current needs for National Policing but will need regular review to ensure its remains relevant for Policing needs.