Document Name	**National Policing - Accreditation Policy**
File Name	National Policing Accreditation Policy v2_0.doc
Authors	David Critchley, Dave Jamieson and Antony Holland
Reviewer	

Authorisation	Police Information Assurance Board
Signed version held by	National Police Information Risk Management Team (NPIRMT)

For additional copies, or to enquire about the content of the document, please contact NPRIM at information.assurance@homeoffice.pnn.police.uk

Table of Contents

Aim and Purpose

The Accreditation Policy sets out the National Policing information assurance and accreditation standards, and expectations relating to the accreditation of National Information Systems. It also embeds proportionality and accountability into the accreditation process.

Scope of Policy

This policy applies to all Police National Information Systems and services, as defined below and in Ref [1], in support of United Kingdom Police forces/agencies.

Accreditation

Accreditation can be defined as a formal, independent assessment of an ICT system or service against its IA requirements, to ensure that the residual risks, in the context of the business requirement, are identified, managed, and acceptable to the business[1].

Accreditation is a mandatory business process for all Police National Information Systems that hold protectively marked or other sensitive police information. It is mandated by the National Policing Information Systems Community Security Policy (CSP) Ref [2], and the Security Policy Framework (SPF) Ref [3]. It is also a requirement of the National Policing Community Code of Connection Ref [4]

Definitions

The following definitions are used in this policy document:

A National Police Information system is:

- The system must be one, which is provided for the Police community as a whole and managed centrally[2], and
- It must be used by a number of forces (at least 10), and
- Police ICT Directorate and/or PNC Services of the Home Office have a contractual relationship with the service provider and/or the service management of the system.

Proportionate approach: i.e. the effort required to accredit a system should reflect its complexity and level of risk. This is reflected in the depth of documentation that is generated, as well as in the level of controls and assurance implemented to mitigate risks.

Accountable: i.e. the delegation of responsibilities and communication of risks. Individuals must be aware of their responsibilities regarding

[1] Good Practice Guide 47 - Information Risk Management (Section 162).

[2] Managed centrally makes the distinction that the system is not distributed (e.g. PNC which is hosted and administered centrally) or a distributed system, hosted and managed at individual force level (e.g. Holmes 2). A system in a cloud environment which is centrally administered is considered a centrally managed system.

information risk, and must make explicit risk management decisions. They must recognise their responsibility for those decisions, which may include appropriate communication.

Governance Framework

National Policing has mandated, through the CSP, the accreditation of police ICT services to manage risks to police information held in National Information Systems. The accreditation service for National Information Systems is provided by the National Police Information Risk Management Team (NPIRMT) on behalf of the police service. the accreditation policy and its supporting processes are incorporated within the National Policing IA Governance structure which is shown in the following diagram (Figure 1):

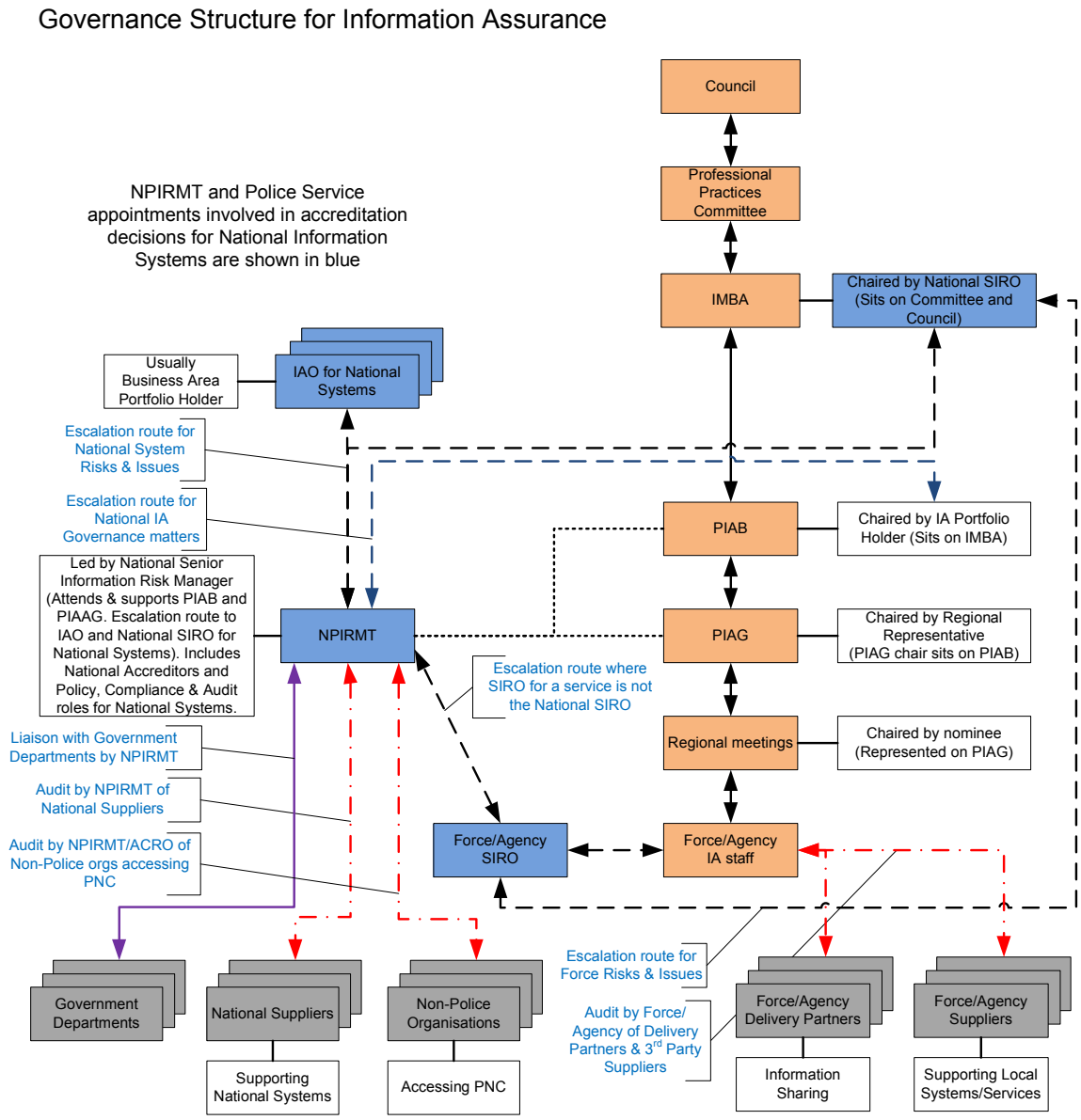

Figure 1- National Policing IA Governance

Further details of the National Policing IA Governance structure can be found in the current version of the National Approach to Information Assurance, Ref [5].

Each national system, in order to be accredited, requires a National Accreditor to be assigned. The Lead Accreditor (National Accreditation Manager) will assign an Accreditor on the basis of the system accreditation requirements. This encompasses delegated authority for accreditation and accreditation decisions, for which the assigned Accreditor is accountable.

The business retains responsibility for coordinating the accreditation process; therefore the product/project lead should assign an individual as the accreditation lead for the product/project who will have responsibility for ensuring the accreditation processes are followed.

Accreditation ensures the residual risks are known, understood and communicated through the IA Governance structure reflected in figure 1, for acceptance at the appropriate level. Ultimately police information is owned by National Policing, and the risks to it are owned by the National SIRO. However, in certain circumstances a national system may have a different SIRO. In either case the communication and escalation of risk must reflect the governance framework appropriate to the system

Risk management for systems under the remit of the National SIRO may be delegated to the SRO/IAO of the National System and the National Accreditor. Each can accept a level of information risk on behalf of the National SIRO. Where systems are not under the remit of the National SIRO, all residual risks must be escalated to the relevant SIRO and Information Asset Owner (IAO) for acceptance.

In either case, the residual risk must be communicated to the National SIRO and/or IAO. Residual risks will be communicated using the National Risk Statement (covering all national systems), and Accreditation Summary (for individual systems).

Accreditation Processes

Accreditation processes are an integral component of all National Information Systems and the National Accreditation Manager should ensure there is an appropriate level of oversight and direct involvement of a National Accreditor in all National Information Systems.

Other processes are detailed in the Accreditation Requirements across Projects/Live Services below.

Accreditation Requirements across Projects/Live Services

Service/project managers must ensure there is Accreditor involvement at project start-up meetings. The Accreditor will define the IA deliverables for a project/service. These may include:

- Business Impact Assessment;
- Privacy Impact Assessment;
- Technical Risk Assessment;
- Risk Management & Accreditation Document Set (RMADS);
- Code of Connection;

- Data Interchange Agreement;
- IT Security Health Check (ITSHC) – CHECK Scheme;
- Data Protection Compliance Check.

Service/project managers will be required to oversee and resource a Business Impact Assessment (BIA) to identify the Business Impact Levels (BIL) associated with the new service. The Accreditor is to be involved in the BIA process. A Privacy Impact Assessment may also be required.
Where the service being developed is complex[3], the Accreditor will advise the service/project manager whether a snapshot technical risk assessment is required to influence the design of the service.

The service/project manager should resource IA staff within their team. The IA staff may include an IA architect and/or IA analyst and this must be built in to the project resource plan.

The Accreditor will support the service/project IA staff through the threat assessment and agreeing the baseline for the risk assessment.

Service/project IA staff may request the addition of additional Threat Sources, Threat Actors, that reflect the unique circumstances surrounding the introduction of the service being accredited. All such additions must be agreed with the Accreditor, any additions/amendments or omissions from the National Information Threat Model [Ref 9] must be documented along with the rationale for the change.

Service/project IA staff will be required to include Forms 1 to 6 of the IS1 technical risk assessment. Depending on the complexity of the system and level of risk associated with the service to be accredited a composite Form for risk treatment may be acceptable. This will be determined by the Accreditor. The Form chosen must provide a means of tracking risks from initial identification to treatment.

The Accreditor will confirm to the service/project IA staff to what extent a completed Baseline Control Set will be required.

The Accreditor must retain a degree of independence; although not responsible for the design of a system an Accreditor can comment on the suitability of system designs and associated changes from an accreditation perspective, and offer advice on accreditable solutions.

It is mandated by National Policing for a Security Working Group (SWG) to be established for National Information Systems and the Accreditor should be included as a member of this group. SWGs must be in place, to progress and resolve IA issues. The SWG must be suitably resourced by the project/product team.

Project/Programme teams (via their accreditation lead) shall provide the Accreditor with the appropriate information necessary to effectively carry out their duties in alignment with the Accreditation Guidance, Ref [6].

[3] E.g. A complex system may be one with high complexity with multiple data feeds and interfaces, or, connections to all Forces, or, multiple connections to external non-Police entities, or, a service offering Internet facing services to the public.

Project/Programmes shall provide an appropriately detailed RMADS for the service, which follows HMG and Police standards, incorporating a technical risk assessment based on the standard methodology (currently reflected in HMG IS1& 2, Ref [7]). The RMADS must be based on actual configurations/implemented policies and processes (i.e. known facts) rather than aspirations.

The detail required within the RMADS for each system shall be agreed with the system Accreditor[4]. Changes to systems may require a review of the level of detail necessary and the Accreditor may require further information as circumstances dictate. Details of National Policing Vetting Policy clearance and physical security assurance should always be included where appropriate or agreed with the Accreditor.

Systems shall use the Modular RMADS template as the basis of any new RMADS produced. Deviation from this standard will be discussed and agreed with the system Accreditor at the earliest opportunity.

RMADS shall need to be maintained by the Project/Programme/Service delivery team throughout the lifetime of the service. It is the responsibility of the Project/Programme/Service delivery team to ensure the RMADS are maintained in line with Accreditation standards and are delivered to the system Accreditor for review in line with re-accreditation timescales.

As a minimum, the project/product team will ensure the risk assessment of a system and the BIA are reviewed on an annual basis. All updates to an RMADS shall be completed in a timely fashion prior to the Accreditation review date to ensure continued Accreditation coverage for the service.

Relationships with Commercial Organisations

Development, implementation, hosting and management of Police ICT systems are very often outsourced to third party suppliers. Where this is the case, Security Aspects Letters (SAL) must be used to communicate the Business Impact Levels associated with the data. Security Aspects Letters must be signed by the contracted organisation as well as the originating Authority.

The procuring project must ensure that security requirements are included in the contracts, which should also reference the SAL.

During the term of a contract, the procuring project must ensure that the security requirements of a contract are being delivered by the supplier. Assurance in compliance should be sought. SWGs (mentioned above) are a key mechanism for establishing such assurance.

Where third party suppliers are used, the business will use appropriate Information Assurance auditing standards to ensure compliance, such as Information Assurance Maturity Model (IAMM), Supplier Information Assurance Tool (SIAT) and/or ISO 27001.

[4] A system Accreditor is the National Accreditor assigned to the system by the National Accreditation Manager.

Legacy Systems & Services

The IRM approach for legacy systems and services is particularly challenging as typically most legacy systems or services will predate the latest National Security Policy, IA Standards and guidance. Indeed it is likely that legacy systems or services would not be able to meet National Security Policies, IA Standards or guidance; this is because of the age of the associated technologies, limited functionality and/or architecture.

Legacy systems will be subject to risk management and acceptance against the current IA Policies. This could be a snap shot technical risk assessment as a minimum. The IA deliverables necessary to renew the accreditation of a legacy system will be determined by the Accreditor.

It is appreciated that risk treatment may be limited due to the age, limited functionality or interdependencies of the legacy system and this will be taken in to consideration in the acceptance and continued use of the legacy system. There may be an increased emphasis on risk acceptance over risk treatment for such systems, at the discretion of the Accreditor and the IAO.

Dynamic Systems & Services

This covers rapidly or constantly changing hardware systems, where the production of full RMADS documentation may be cumbersome given the pace of change. These situations must be negotiated with the Accreditor. Possible approaches include establishing a baseline RMADS and Accreditation, and accommodating the planned changes under change control and documenting them through a series of addenda, each approved by the Accreditor in line with the scheduled delivery. Another approach may be to accredit in milestones, with documentation to support each milestone.

Accreditation Scope

National Information Systems accreditations have a defined scope, in order to achieve a manageable accreditation strategy across the landscape of police systems and networks. The accreditation scope must be defined early on in the accreditation process, to avoid duplication and to identify gaps in accreditation, i.e. where systems or parts thereof have not been accredited.

The Accreditor will work with the service/project IA staff to ensure the accreditation scope, reliance scope and overall assessment scope for the service is identified and understood. The scope of an Accreditation may be modified under change control and agreement with the Accreditor.

The scope of accreditation must be defined and understood in order to enable proportionate accreditation and to understand the interdependence of system accreditations to ensure adequate coverage but avoid duplication of effort.

Interconnections

Through interconnections and interfaces, systems and networks present risks to each other. These risks must be captured during the accreditation process.

However, external systems and networks may change, or new connections may be introduced - and the level of threat to the National Information System therefore may be increased. Where the assurance associated with community or connected networks is reduced (e.g. through replacement or migration to networks with lower levels of assurance), the risk posed by such networks to National Information Systems is increased. This could prompt a review of risks and potentially re-accreditation.

System owners, service delivery/project managers and Accreditors must recognise the interdependence of information system risk. System 'owners' must remain aware of the external environments to which their systems connect, and inform the Accreditor of any changes to the threats or risks to the national system that might require review or re-accreditation. Codes of Connection are often used to manage these interdependencies.

In particular, for those organisations applying to gain and retain access to police community networks and information systems, the CSP mandates compliance with the Community Code of Connection to manage the risks associated with the connecting organisation.

Re-Accreditation Conditions

Accreditation is a continual process and requires annual review of the risks. Within the period of accreditation, accreditation is dependent on the defined scope and risk profile remaining the same. Therefore a review of accreditation will be required when significant changes to the system are put in place.

Changes may include:

- Significant changes to the systems components or architecture.
- Changes to User Clearance Status
- Significant changes to any risk component (including the impact levels /protective marking of the information and/or threat landscape)
- The business use or governance changes
- Changes in the volume of data
- The accreditation audit report indicates significant concerns
- Changes to the system location
- Changes to system interfaces/connections
- Changes to system functionality
- Any identified system / process weakness
- Any changes to procedures including changes to documentation

Accreditation Patterns and Templates

Accreditation patterns are not currently used for police accreditation.

The Modular RMADS template should be used for generating new RMADS documentation. This can be used for a single RMADS or for generating a Cardinal-Subordinate set of RMADS, to facilitate a proportionate approach to accreditation.

Policy Ownership and Comms Strategy

This Accreditation Policy is owned by PIAB and maintained by the NPIRMT under its mandate. It will be promulgated through ACPO Intranet and POLKA for Police IA Community members.

Links and References

[1] Definition of a National System (PIAB Approved 24th July 2012) (Published on POLKA IA Community Pages).
[2] National Policing Community Security Policy (CSP) (Published on POLKA IA Community Pages).
[3] HMG Security Policy Framework (SPF) (Published on Cabinet Office Website).
[4] National Policing Community Code of Connection (Published on POLKA IA Community Pages).
[5] National Policing National Approach to Information Assurance 2014-2017 (version 0.3 DRAFT, dated 15th November 2013).
[6] NPIRMT Accreditation Guidance (Published on POLKA IA Community Pages).
[7] HMG IS1& 2 (Published on CESG Secure Website).
[8] NPIRMT mandate (Published on POLKA IA Community Pages).
[9] National Information Threat Model (NITM) (Published on POLKA IA Community Pages)

This policy is governed by:

- HMG (CESG) Information Assurance Standard 1&2
- Good Practice Guide 47 Information Risk Management
- HMG SPF
- National Policing CSP

Associated documents include:

- IA Governance Framework
- National Risk Appetite Statement

Accreditation Register

The National Accreditation Manager tracks the accreditation status of all National Police ICT systems and services, which is made available to National Policing via the Police Information Assurance Board.

Review

This Policy should be reviewed on an annual basis or as required to remain consistent with National and Police IA policy.