Document Name	**Accreditation guidance**
File Name	Accreditation guidance v2_6_Final.doc
Authors	Antony Holland

Authorisation	
Signed version held by	National Policing Information Risk Management Team (NPIRMT)

For enquiries, please contact the NPIRMT on
information.assurance@homeoffice.pnn.police.uk

Table of Contents

1 Controlling documents

This section contains reference to any source material used in the preparation of the document.

Ref No.	Description	Document number	Revision
1.	HMG Security Policy Framework Tiers 1-3	V11	Oct 2013
2.	HMG Security Policy Framework Tier 4	V11	Oct 2013
3.	ACPO/ ACPOS Information Systems Community Security Policy	V4.0	May 2012
4.	ACPO/ACPOS Information Risk Management Guidance (see Police IA Functions and Responsibilities section)	V1.1	Dec 2011
5.	HMG IA Standard No 1&2: Information Risk Assessment	V4.0	Apr 2012
6.	HMG IA Standard No 1& 2 Supplement: Technical Risk Assessment and Treatment	V1.0	Apr 2012
7.	National Threat Model for the police service	V1.2	Oct 2013
8.	Community Code of Connection	V3.3	Apr 2013
9.	ACPO Vetting Policy	V3.0	Aug 2010
10.	GPG47 Information Risk Management	V1.0	Apr 2012
11.	ACPO Letter Signed 20 Sept 2012 re SRO and IAO National Systems.doc		Sep 2012
12.	National Systems Definition – (on POLKA)	V1.0	Jul 2012
13.	Guidance on the IAO Role (on cabinet website)	V1.2	Oct 2013
14.	Accreditation Policy	V1.0	Oct 2012

2 Introduction

2.1 Purpose of document

2.1.1 The purpose of this document is primarily to provide guidance to Accreditors, Information Assurance (IA) professionals and project/programme managers in relation to the accreditation of police Information Systems, and the processes required within the Police community. It is primarily intended for national systems but it can be used by local Force/Agency[1] IA staff for local accreditation processes.

2.1.2 Accreditation is a formal governance process defined in CESG guidance, grouped into the CESG IA Policy Framework. Further information may be found in HMG IA Standard No 1&2 [refs 5 & 6], and GPG 47 [ref 10].

2.1.3 As the IA Policy Framework is updated regularly, this document should be reviewed periodically to capture any changes and their impact on the Accreditation processes as relevant to the Police Service. Similarly, documents produced to comply with the Accreditation process should be checked annually against the IA Policy framework to ensure it is compliant with changes in policy.

2.2 Background

2.2.1 Accreditation is a mandatory business process for all Police Information Systems that hold protectively marked information. It is mandated by both the ACPO/ACPOS Information Systems Community Security Policy (CSP) and the Security Policy Framework (SPF)[2].

2.2.2 Accreditation is an independent assessment of information risks and the degree to which they are mitigated and managed in line with the business requirement. It therefore determines whether an information system meets its IA requirements and whether the residual risks, in the context of the business, are acceptable to the relevant senior business risk owner. IA requirements defined in the Security Policy Framework provide a basis for this assessment.

2.2.3 The principle of Accreditation is to ensure risks associated with information are being properly managed, with the aim of sufficiently protecting Confidentiality, Integrity and Availability of Police information to a level acceptable to the business.

[1] For the remainder of this document the term 'Force' will be used to refer to any Force/Agency required to Accredit information systems according to the police service Accreditation process

[2] The Security Policy Framework is mandatory for all organisations following the government protective marking scheme.

2.2.4 Accreditation forms part of the overall governance of an information system. It helps to ensure security risks are understood and managed throughout the entire life cycle of a service.

2.2.5 Security (Information Assurance) is more effective and cost efficient when it is inherent to the design and implementation of a system. The process of accreditation embraces the best practice approach of project implementation alongside established risk management to ensure that security is an integral component of a system from the outset rather than 'bolted on' during or after acceptance into service.

2.2.6 Normally, all central government information systems (including those operated on behalf of the Police service) holding protectively marked information must be accredited. For the wider public sector, the accreditation process is recommended for any information system or service where the loss or compromise of that system or service would adversely affect business capability or integrity. Chief Constable's council has mandated accreditation for all systems used in operational policing, and this is reflected in the Accreditation Policy [ref 14].

2.2.7 An information system is deemed to be accredited when the Accreditor determines that the physical, personnel, procedural and technical countermeasures are sufficient to reduce the residual information risks to a level acceptable to the business.

2.3 Structure of document

2.3.1 This document is comprised of the following sections:

- Section 3 provides a review of the functions within the Accreditation process;
- Section 4 describes the process and lifecycle of Accreditation;
- Section 5 describes the development of an RMADS and supporting evidence
- Section 6 is intended for Project Managers and covers the stages within a project life cycle (based on the Office of Government Commerce Gateway process) and the expectations of an Accreditor for information required as part of an Accreditation.
- Section 7 is an aide memoire for project managers responsible for managing accreditation.

3 IA Functions/roles and responsibilities

3.1 Purpose of this section

3.1.1 This section provides a summary of the key functions and responsibilities of the various individuals /stakeholders that may be involved in the Accreditation of an Information System.

3.1.2 The nature and functions outlined below, may be subject to individual organisational requirements, thus the following are to be used as guidance. However, the functions performed will still need to be fulfilled by some entity within the organisation in line with the requirements of the Information Systems Community Security Policy.

3.2 Senior Information Risk Owner (SIRO)

3.2.1 The Senior Information Risk Owner (SIRO) has responsibility for IA governance and risk ownership in the organisation. Specifically, the role of the SIRO is to understand how the strategic business goals of the organisation may be affected by failures in the secure use of the organisation's information systems, and to ensure that these information risks are managed.

3.2.2 There is a National SIRO who makes risk management decisions on behalf of the police that relate to shared police information. Forces will each have a Force SIRO that makes similar decisions about the data that is owned and used solely by that force.

3.3 Information Asset Owner (IAO)

3.3.1 This role is defined in the Cabinet Guidance on the IAO role [ref 13]. The IAO has accountability for the information risk associated with live data, ensuring that the information asset is effectively managed.

3.3.2 As such, there should be an IAO accountable once live data gets introduced and the data is protected appropriate to the risk appetite/acceptance of the specific IAO.

3.3.3 As part of their review of information risks, IAOs are responsible for ensuring that the information systems assigned to them have current accreditation, and undergo re-accreditation within an appropriate timeframe.

3.3.4 ACPO has nominated an Information Asset Owners for each national system. The list is available at [ref 11].

3.4 System/Product/Project Manager

3.4.1 It is the responsibility of the System/Product/Project Manager to achieve and maintain accreditation for their information system.

This will involve getting the appropriate resource to manage accreditation, identify IA requirements and author the RMADS[3].

3.4.2 As such the project manager/product manager are responsible for ensuring the Information Asset owner is making informed decisions about risk and risk acceptance.

3.4.3 They must remain aware of the external environments (i.e. other systems) 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.

3.4.4 It is noted that Project Managers may cease to be involved in an information system following its delivery into live service. It is therefore their responsibility to ensure that the live system has an owner with responsibility for gaining re-accreditation prior to the expiry of the Accreditation Certificate.

3.5 Information Security Officer (ISO)

3.5.1 The ISO is responsible for development and implementation of Information security policy and procedures within their Organisation in accordance with:

a) The Security Policy Framework issued by the cabinet office;
b) HMG technical security standards issued by CESG, the National Technical Authority for Information Assurance;
c) ACPO/ACPOS Information Systems Community Security Policy (CSP); and,
d) The business needs of their Organisation.

3.5.2 These actions would normally be undertaken in conjunction with senior security staff, the Force/Agency SIRO and those responsible for IT services (including Managed Service Providers).

3.5.3 The ISO is also responsible for:

- Involvement in organising IT security;
- liaising with National Police Information Risk Management Team (NPIRMT), HMG security and IT authorities on local and National Security policy issues;
- Providing advice on security reviews and investigations relating to information security issues; and,
- Information security awareness education and training.

3.5.4 In some instances the role of the ISO and the Accreditor may be combined. Should this occur, the impartiality of the Accreditor function must be maintained.

3.6 Accreditor

[3] Advice in procuring a CLAS consultant with the appropriate skill set may be sought from the NPIRMT (although forces will be responsible for their own procurements).

3.6.1 The role of an Accreditor is to act as an impartial assessor of the risks to information systems. Their function is to assure that systems are sufficiently secure to be placed into, and to continue to function in, operational service. They accredit systems on behalf of the SIRO.

3.6.2 Within the Police community there are both Force Accreditors and National Accreditors.

- The role of the Force Accreditor is to review the level of residual risk within the force and to either accredit the Force local systems or escalate the risks to the Force SIRO, according to the risk appetite of the force. The Force Accreditor also accredits the local force network, which can be reviewed by the National Accreditor for approval to connect to national systems and networks. Force Accreditors may also accredit regional or shared systems which do not qualify as national systems [ref 12].

- The role of the National Accreditors is to review the level of residual risk of National Police systems (as defined in ref [6]). They also accredit Force connections to national services (including the CJX) to ensure that they meet national standards for connectivity. The National Police Information Risk Management Team (NPIRMT) undertakes the Accreditation of National Police Systems (as defined in [ref 12] under the remit of the National SIRO for the Police service.

3.6.3 Force or National Accreditors will either accredit a system or escalate the remaining residual risks above the Police Service risk appetite to the relevant Information Asset Owner or SIRO. This is explored further in the sections 4.3 and 4.4.

3.6.4 The Accreditor will provide accreditation support and advice throughout the lifecycle of the project. This is to prevent developments that may make accreditation of the service difficult at a later date. The intention is that all systems going live are sufficiently secure for the business needs. However, to keep the impartiality of their function within the Accreditation process, there are certain activities that an Accreditor cannot help a project with.

3.6.5 An Accreditor will:

- Agree the scope of the Accreditation.
- Provide advice and guidance on the risk management and accreditation requirements of an information system throughout its lifecycle;
- Provide guidance on the content, preparation and upkeep of the Risk Management and Accreditation Document Set (RMADS);

- Approve the RMADS, including all changes, throughout the system lifecycle[4];
- Specify assurance requirements and standards that apply to the target information system;
- Be responsible (through inspection) for ensuring that assurance requirements and standards have been implemented.
- Advise on the scope of an IT Health Check and the suitability and priority of proposed remediation(s).

3.6.6 An Accreditor will not:

- Be the author of, nor responsible for the upkeep of the Risk Management and Accreditation Document Set (RMADS);
- Act as the technical design authority for the proposed information system; or,
- Act as the technical security resource for the proposed information system.
- Be involved in routine day-to-day decisions

3.6.7 However, under exceptional circumstances an Accreditor may find that there is a strong enough business reason to step over the boundary of impartiality and support a project with one or more of the responsibilities as identified in the previous paragraph.

3.6.8 An Accreditor has the responsibility of ensuring that information systems do not put the organisation at an unacceptable level of risk. However, it is appreciated that the process of Accreditation can be seen as a burden on the delivery of services. To ensure that this perceived burden is minimised an Accreditor will work as closely as possible with project and programme managers to make the whole process of Accreditation as smooth and seamless as possible.

[4] This includes staged approval, as appropriate, of the various sections or documents

3.7 IT Security Officer (ITSO)

3.7.1 The Force may have an ITSO. The ITSO role is usually located within the IT department and is responsible for ensuring that IT security is implemented effectively, co-ordinating the technical aspects of protective monitoring, security incident investigations and change control. The ITSO role may also include the provision of security technical support and support in the development of Risk Management Accreditation Document Set (RMADS) for systems that have to undertake accreditation.

3.8 Operational Security Manager (OSM)

3.8.1 The OSM role is responsible for management/escalation of security issues for one or many systems. The responsibility covers all technical and procedural aspects of security and to some extent physical security. It includes:

- Development and implementation of security procedures
- Support to projects/future systems
- Examination of CJX IDS reports
- Policing supplier implementation of protective monitoring
- Approver for change requests
- Chair/Deputy chair of various Security Working Groups
- Review, comments and acceptance of Code of Connection (CoCo) and Compliance documents from suppliers
- Recipient of security incident reports within agreed timescales and management and/or escalation of such incidents as necessary
- Trusted advisor to Accreditor. Responsible for system meeting accreditation requirements.
- Involvement in Incident Management, Change Management and Problem management
- Auditing of suppliers and users of the system
- Advice and guidance on incident management to suppliers
- Advice and guidance on resolution of problems, occasional identification of underlying trends
- Attendance at Change Management bodies and service review meetings

4 The Accreditation Process and Lifecycle

4.1 Purpose of this section

4.1.1 This section of the document aims to help explain the Accreditation process. The information provided here relates to the process used for the Accreditation of National systems for the Police service. The same process can be used for accreditation of local systems by Forces. This process is based on that detailed within IAS1&2 [ref 5 & 6] and conforms to the ACPO/ACPOS Accreditation Policy [ref 14].

4.2 Accreditation of New Systems

4.2.1 Accreditation forms part of the overall governance of an Information System and should not be viewed as a "point in time" exercise happening at the end of the system development lifecycle.

4.2.2 It is best practice to involve the Accreditor from the very beginning of the project lifecycle, with regular communications between themselves, the Project Manager, Information Security Officer and CLAS consultant(s) if used.

4.2.3 The aim should be to involve an Accreditor as early as possible within an information system's life cycle. For solutions procured it SHOULD be during the procurement process, for in house solutions this SHOULD be during the early concept stages.

4.2.4 At an early stage of the system development an initial ('snapshot') risk assessment will normally be recommended by the Accreditor. This will help to focus the design decisions of the final solution.

4.2.5 Whilst a system is being developed and implemented the project team can start the RMADS development.

4.2.6 During the development of a solution it is the project manager's responsibility to ensure that appropriate controls get implemented to ensure that the data is protected. There should be an Information Asset Owner accountable for the data on the system who will determine whether the risks are acceptable.

4.2.7 Generally during system testing, non-live data should be used, and in particular the use of personal data should be avoided. The Accreditor should be consulted if there is a strong and valid business reason for using personal data during testing.

4.2.8 It should be recognised that the code developed for a system (as well as the technical design and specifications) may attract a Protective Marking. Development (and Test) Environments may need to be accredited themselves.

4.2.9 RMADS development will continue through the stage where the system undergoes an IT Health Check (ITHC), using certified

CHECK testers[5]. Output from the CHECK assessment, together with any remedial action undertaken by the project team to reduce the vulnerabilities identified, will be incorporated into the RMADS.

4.3 Accreditation Decision

4.3.1 An Accreditation Decision is generally made on the basis of residual risk to the system and the information on it. The Accreditor will review the completed RMADS to see whether they are complete and provide sufficient evidence for an accurate assessment of residual risk.

4.3.2 If he/she finds the RMADS lacking in critical detail, for example related to risk assessment or risk management, further information will be requested. If the RMADS is lacking some details which appear to be non-critical to the overall security of the information system, the Accreditor may still make an accreditation decision based on the risks. The project/product team would generally be given a specified time limit to work on rectifying the issues identified by the Accreditor and produce an acceptable RMADS.

4.3.3 With an acceptable RMADS the Accreditor will assess whether the security mechanisms identified sufficiently mitigate the risks to the system to bring the residual risk within the risk appetite of the organisation (See 4.4).

4.3.4 Should the Accreditor decide that a system can be accredited they have two possible options:

- Interim Accreditation; or,
- Full Accreditation.

4.3.5 The Accreditor may suggest Interim Accreditation. This occurs when there are deficiencies that can be remedied within a reasonable timeframe and agreed as action by the project in an Accreditation Plan.

4.3.6 **Interim accreditation** will therefore likely include a set of conditions with limited timescales. For example an Accreditor can support the business with an interim accreditation by acknowledging some additional risk for short term – with agreement of business to meet the Accreditation conditions.

4.3.7 The Accreditor may suggest **Full Accreditation**. This will occur should the Accreditor believe that risks are currently being managed to an acceptable level.

4.3.8 When a system is accredited the project/product manager will be responsible for having an Accreditation Summary for the system

[5] The ITHC is a process where a system is assessed for technical security vulnerabilities and is a scheme run by CESG. See http://www.cesg.gov.uk/servicecatalogue/CHECK/Pages/index.aspx

produced. An Accreditation Summary report captures the residual risks for discussion with the Information Asset Owner (IAO. If the IAO is willing to accept the residual risk the Accreditor will provide an Accreditation certificate (either Interim or Full) for the system. Accreditation reviews will then continue throughout the in-service life of the system until it is decommissioned.

4.3.9 Under certain circumstances the Accreditor may not be able to accredit a system, yet there is a business imperative to go live. For these extremely exceptional circumstances an escalation process exists. This process should lead to the Senior Information Risk Owner (SIRO) making a risk management decision, which may be accepting the risk and allowing a system to go live. This is referred to as **Approval to Operate**.

4.4 Risk Appetite

4.4.1 Residual risk is the level of risk perceived to exist after security controls have been implemented to reduce the risk initially identified in the risk assessment. Residual risk is minimised through countermeasures and checks that the countermeasures are in fact implemented correctly and effectively.

4.4.2 The initial risks identified during the risk assessment are measured on a scale from Very Low to Very High; application of security controls will result in these risks being reduced by varying degrees to provide the residual risks. This reduction is a matter of professional judgment by the project's IA Advisor and agreed by the Accreditor, informed by CESG guidance on Risk Treatment.

4.4.3 The residual risk will then be compared with the risk appetite, using the delegation matrix[6] identified in the National Risk Appetite statement to identify the appropriate level of risk acceptance.

4.4.4 In exceptional circumstances a system may have a Risk Tolerance statement that assigns the system a risk appetite that deviates from the National Risk Appetite. If this exists and has been signed off by the National SIRO, the relevant table for the risk appetite for the system will be used.

4.4.5 If the residual risk still exceeds the appetite for the organisation there may still be a business imperative for the system to become operational. If this is the case the Accreditor will discuss with the project team as to what options are available to improve the situation. This may lead to changes to the design and implementation and/or the inclusion of additional security measures to sufficiently mitigate the risk.

4.4.6 If the residual risk remains above the risk acceptance of the Accreditor, the Accreditor will work with the project to help them

[6] The delegation matrix in a Risk Appetite statement indicates the roles who are able to sign off a risk as acceptable according to the risk appetite.

develop a Risk Escalation Case which is generally escalated to the IAO or SIRO[7]. With a sufficiently robust Risk Escalation Case the IAO or SIRO may agree to accept the risk, in which case the Accreditor may accredit the system.

4.4.7 The Accreditor will also review the assurance that the specified controls are indeed in place (and not just on paper). This will use a particular input in the RMADS called the Residual Risk Indicator. If insufficient assurance exists then the Accreditor will decide whether to escalate this through the IAO to the National SIRO.

4.5 Reaccreditation

4.5.1 Systems will require reaccreditation when there is a significant change to a system, or annually, as defined in 6.2.20.

5 Developing IA requirements and the RMADS

5.1 Overview

5.1.1 A key component of the Accreditation process is the Risk Management and Accreditation Document Set (RMADS). This document, or set of documents, provides a comprehensive picture regarding an information system and its risks. An Accreditor uses this document/document set as the primary source of information in the assessment as to whether a system is suitable for operational service. Details as to what information that should be included within and RMADS is identified in HMG IA Standard IS1&2. RMADS templates can be requested from the NPIRMT.

5.1.2 There is an ongoing drive to be proportionate about accreditation, in terms of the effort and documentation required to accredit a system. The Modular RMADS template reflects a proportionate approach to accreditation, since subordinate RMADS can refer back to the main (Cardinal RMADS) to reduce duplication.

5.1.3 Anyone undertaking the writing of an RMADS should have a strong understanding of HMG Information Assurance standards. It is therefore highly recommended that those with a specialism within this area (ITPC Practitioner or CLAS consultant) be employed whilst undertaking such a task

5.1.4 The following sections discuss the precursors to an RMADS.

[7] A template and supporting guidance for writing Risk Escalation Cases is available from the NPIRMT.

5.2 Business Impact Assessment

5.2.1 A precursor to the development of an RMADS is the assessment of the Business Impact Level (BIL) of the system and its data. This is done through a Business Impact Assessment (BIA) which looks at three aspects:

- **Confidentiality (C)** – the sensitivity of information held by the system;
- **Integrity (I)** – the accuracy of information held; and,
- **Availability (A)** – the operational availability of the service.

5.2.2 The potential impact of the loss in one, or more, of these three aspects is assessed against a set of business impact assessment tables within the HMG IA Standard IS1&2. The tables of primary interest for police systems will be Table 2 relating to Public Order, Public Safety and Law Enforcement, although impacts from other tables may also be applicable. This will result in an identification of a BIL between 0 and 6 for each of the aspects. In the majority of cases Police systems have a higher requirement for Availability and Integrity to support intelligence-led policing. Guidance can be sought from the NPIRMT on the application of BIL to police information.

5.2.3 The higher the levels of C, I and A identified in the BIA, the higher the level of controls are likely to be needed to ensure the capability of the solution to sufficiently mitigate risks.

5.3 Privacy Impact Assessment

5.3.1 A third precursor document that may be required is a Privacy Impact Assessment[8]. This assesses a system against the Data Protection Act. The outcome of the assessment may influence the security mechanisms required by an information system and have an impact on the Accreditation of the solution.

[8] Instructions for completion of PIAs can be found at the ICO website http://www.ico.gov.uk/for_organisations/topic_specific_guides/pia_handbook.aspx

5.4 Confirm Risk Appetite/Risk Tolerance

5.4.1 At an early stage of the system conception, a risk tolerance will be confirmed for the system. The risk tolerance for national systems or systems connected to national systems is likely to be inherited from the National Risk Appetite statement[9]. Local systems inherit a risk appetite/tolerance from the Force/Agency Risk Appetite statement. The national/local risk appetite and the risk tolerance for the system should be reflected in the RMADS.

5.4.2 At this stage a risk tolerance statement may be submitted to the Accreditor to have the system's risk appetite diverge from the National/Organisational Risk Appetite on the basis of the system context. The risk tolerance is not directly linked to the business impact levels for the information system. A greater tolerance for risk must be signed off by the appropriate National or Force SIRO.[10]

5.5 Risk Assessment

5.5.1 An additional precursor to the development of a full RMADS is a risk assessment in line with IS1&2 to identify potential Threat sources[11], Threat Actors[12] and Risks[13], as well as risks from Accidental Compromises. This risk assessment will help inform design decisions of the final solution.

5.5.2 The output of a risk assessment should be used with the identification of appropriate Physical, Procedural, Personnel and Technical controls that will help ensure the delivery of a sufficiently robust solution.

5.6 Components of an RMADS

5.6.1 The precursor documents to an RMADS, when combined with a number of other information components, that helps develop an RMADS. Table 1below lists the components of an RMADS, which may be delivered as one document or multiple documents.

- Links and dependencies on other related policies/documents of the organisation (such as corporate business continuity/disaster recovery plans);
- List of applicable legislation (Freedom of Information Act, Data Protection

[9] The National Risk Appetite Statement includes a statement covering National Systems

[10] Guidance on the use of Risk Appetite and Risk Tolerance can be found in the Risk Appetite Framework Guidance document

[11] Threat Sources are persons or groups who are assumed to wish to compromise a systems C, I or A property. Typical examples include Criminals, Hackers and Investigative reporters.

[12] Threat Actors are those that actually undertake an 'attack'. They are the individuals in a position to exploit a particular method to compromise the system, and may do so under the influence of a Threat Source, which may also enhance their motivation and capability to attack. Examples include staff (in various roles), suppliers (where support contracts are in place) and hackers.

[13] A Risk is defined as the potential that a given threat will exploit a give vulnerability of an asset and thereby cause harm to the organisation.

Act, Computer Misuse, RIPA, The Police and Criminal Evidence Act, the Telecommunications Act, and any specific legislation associated with the system under accreditation etc);

- Statement of Compliance/non-Compliance with corporate policies;
- Information on the Accreditation Status of the system, comprising:
  - Accreditation statement (only applicable once system has been accredited);
  - Accreditation History; and,
  - Security Decommissioning Compliance Certificate (only applicable once a system has been decommissioned, or, a technical refresh of hardware, or failure and subsequent replacement of a hardware component).
- Basic information about the system, covering:
  - Business Context of the Information System;
  - Description of the Information System and Assets (including the user community and location of key components as appropriate);
  - Interconnections and Interfaces to other systems;
  - Scope of the Accreditation (what is included and excluded within the Accreditation, it should also identify what is within the Reliance Scope of the service);
  - Responsibilities and Functions (who has ownership of the risk management/security functions and accreditation, along with description of their responsibilities); and,
  - The Accreditation review process of the system (under what conditions a full re-accreditation or an accreditation will be required).
- Information on the Risk Management of the system, comprising:
  - The Corporate Risk Environment (the top level business risks and statement of the organisation's risk appetite);
  - Business Impact Statement (information from the Business Impact Assessment undertaken as a precursor to the RMADS);
  - Technical Threat Assessment
  - Vulnerability Analysis
  - Technical Risk Assessment (based on initial risk assessment completed as a precursor to the RMADS and updated as the system develops);
  - Risk Register (current status of risks); and,
  - Risk Treatment Plan (cross reference between risks and countermeasures of the system).
  - Implementation Plan (detailing the approach to implementing the risk treatment plan)
  - Assurance Plan (how IA assurance will be gained and maintained for the system)
  - Residual Risk Assessment
- Development, Acceptance and In-service (subject to stage within project lifecycle), consisting of:
  - Information Risk Management Plan (a plan, used during the development and into live service of the system, to identify clear milestones and deliverables of Information Assurance management);
  - Results of IA Verification, Testing and Inspections (primarily an IT Health Check report but can include normal testing reports);
  - Security Operating Procedures;
  - Incident Management, reporting, escalation and response (how security incidents will be managed);
  - Assurance Maintenance Plan (how the system will retain its accredited status by such measures as regular IT Health Checks, audits etc); and,
  - Decommissioning and Disposal requirements of the information and assets of the system.

Table 1 Components of an RMADS

5.7 Risk Treatment Plan & Baseline Control Set

5.7.1 A key supplementary component normally associated with an RMADS is the Baseline Control Set, which forms part of the Risk Treatment Plan.

5.7.2 The HMG Information Assurance Standard No. 1&2 Supplement: Technical Risk Assessment and Treatment, Appendix A [ref 6] defines a Baseline Control Set (BCS) and additional controls for mitigating higher risks. The Accreditor will expect to see appropriate compliance to BCS for the system with Business Impact Levels (BIL) of 2 or above (unless there is a documented justification for their omission). These controls should be applied as appropriate according the relevant segment of the segmentation model and may vary due to the specific risk. The Accreditor should be engaged to agree the appropriate segment for the controls being implemented to mitigate the various risks. The application of these controls should be assessed in order to present the residual risk after controls have been applied. The residual risk should be documented in the RMADS for scrutiny by the Accreditor.

5.7.3 It is noted that the degree to which the risk is mitigated is irrespective of the risk appetite. The risk appetite applies to the residual risk, as stated in section 4.4

5.7.4 As the HMG Information Assurance standards are continually being developed and improved additional information may be required in future Accreditations. The Accreditor may request sight of compliance statements of other relevant HMG IA standards/Good Practice Guides/Memoranda as appropriate to the system.

6 Accreditation guidance for Project Managers

6.1 Purpose of this section

6.1.1 This section is targeted at Project Managers. Its aim is to provide guidance in relation to some of the liaison functions, and activities that will be required as part of the accreditation process. This section has been based around the Office of Government Commerce (OGC) model for procuring and implementing a project that was, until a few years ago, the primary model used. Although now dated it provides a structure to provide guidance to Project managers of the deliverables that an Accreditor will expect at the various stages of development of a solution. Project managers will have to adapt this information to their current procurement practices.

6.1.2 Note that connections to national networks (e.g. PNN3/CJX) will also require approval on behalf of the community. This is achieved through the Community Code of Connection [ref 8].

6.2 OGC Gateways and Accreditation

6.2.1 The OGC Gateway Process examined programmes and projects at key decision points within their lifecycle. Its aim was to ensure that programmes and projects could progress successfully to the next stage. The process was seen as best practice in central civil government, the health sector, local government and Defence; for central civil government the OGC Gateway process was mandatory.

6.2.2 Information Assurance standard no.1&2 (Risk Management & Accreditation of Information Systems) aligns the Accreditation process with the OGC Gateway process, providing a model against which project managers can understand how Accreditation fits within the life cycle of projects and programmes. The information in the standard has been reproduced here to support Project Managers in planning Accreditation activities within the overall project life cycle.

6.2.3 The OGC Gateway process, and where Accreditation aligns with a project/programme lifecycle, is shown in Figure 1.

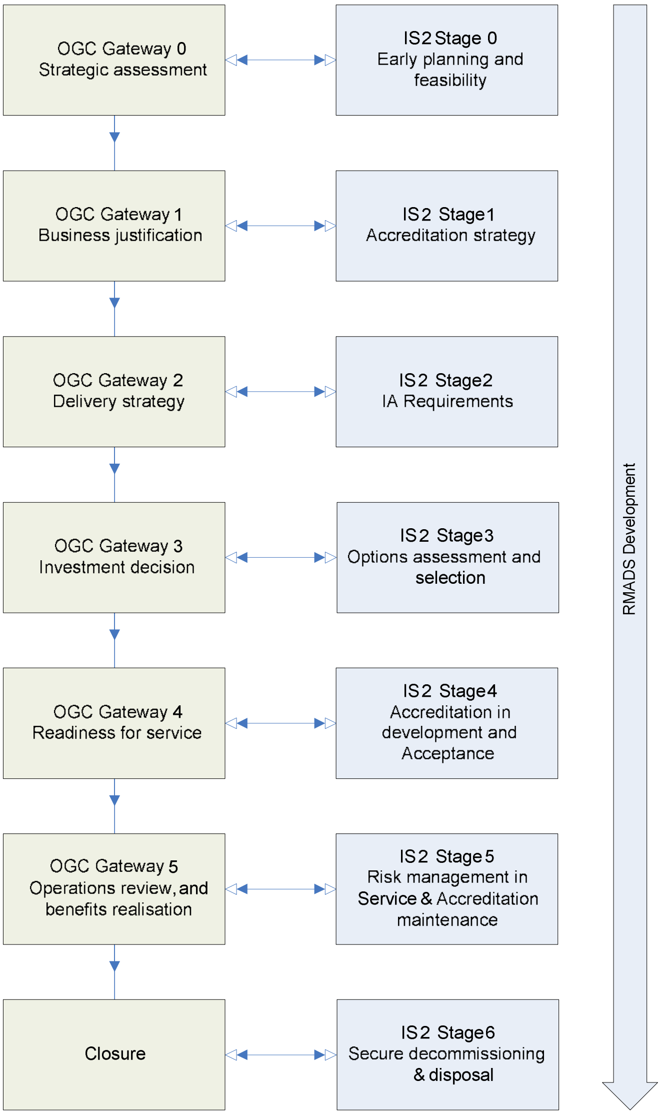

Figure 1 - OGC gateways and the Accreditation process

6.2.4 The following paragraphs identify the Accreditation activities at each stage of the OGC Gateway process.

OGC Gateway 0 – Strategic Assessment

6.2.5 The Accreditation process activities at OGC Gateway 0 (IS 2 Stage 0 – Early Planning & Feasibility) are intended for accreditation of new systems rather than legacy or current systems. As such they are not generally appropriate for re-accreditation. The aim of this stage is to assess the high-level IA risks associated with the business requirement and to provide an early identification of any potential risks to the business plan.

Inputs

- A description of the business requirement, including any relevant business constraints, e.g. costs and time-scales;
- Asset valuation (as determined by the data owners);

- Corporate governance status;
- Applicable corporate IA policies;
- Applicable legislation, directives and IA standards;
- Interconnections that may be required;
- A (high level) threat assessment that relates to the business of the organisation or the service that is being provided;
- Statement of Risk Appetite.

Outputs (System and Accreditation Specific)[14]

- **Business Impact statement**

  An initial Business Impact Assessment of the data being held by the system should be completed. The impact assessment should be conducted utilising the HMG IS1 Business Impact Level tables to determine the protective marking of the data and therefore the level of protection required.
- **Privacy impact assessment**

  Where a system is deemed to be handling Personal Data, a Privacy Impact Assessment must be instigated in liaison with the Data Protection Officer according to the guidance from the Information Commissioners Office to determine the required levels of compliance with the Data Protection act as well as Privacy Laws[15].

6.2.6 It is useful at this stage to start the development of a Risk Management & Accreditation Document Set (RMADS). See HMG IA standard 1&2 for guidance on the contents of a RMADS.

[14] Information used within this stage will be relevant to the overall RMADS. The output listed are those deliverables that are generated in this stage that are specific to this system and are purely Accreditation centric. Other information that is RMADS relevant, such as interconnection requirements, has a broad scope of use within the project/programme.

[15] Legislation of other nations may be applicable should the supplier aim to provide part or all of the provision of the system from a different legislative region.

OGC Gateway 1 – Business Justification

6.2.7 The Accreditation process at OGC Gateway 1 (IS2 Stage 1 – Accreditation Strategy) aims to define an Accreditation strategy for the system that complies with the organisations accreditation standards. If OGC Gateway 0 has not occurred the products from that stage should also be produced during this stage.

Inputs

- Inputs and Outputs of Stage 0;
- Any additional information as available on business options and preferences.

Outputs (System and Accreditation Specific)

- **An initial risk assessment (including risk register and risk treatment plan)**

  The most appropriate source for threat information should be determined in liaison with the ISO/Accreditor. Reference should always be made to the National Information Threat Model [ref 7] for the latest representation of this. The CSP contains high level information about the Threat to information security, while the National Threat Model contains the latest threat profile for the police service. This can be used in the risk assessment approach. Also available from the NPIRMT are guidelines for assessing the Business Impact Levels for police information.

  Consultation with the Force professional standards department, or equivalent, should be made for the most current internal staff threat assessment.

- **Governance Boundary**

  Define the expected boundaries and governance of the information system with a view to identifying any potential issues.

- **Accreditation Scope**

  The Accreditation Scope defines what is within the scope of the Accreditation. It should clearly define the scope for the accreditation, as well as a description of the system, including:

  - Assets (description, quantity, sensitivity);
  - Hardware (main items, with reference to inventory);
  - Software (main items, with reference to inventory);
  - Communications (from/to, purpose, type, sensitivity);
  - People (user groups, roles, organisations, personnel check / security clearances);
  - Locations (may be covered under above headings).

6.2.8 During this stage the identification of specialist resources to support the process (such as the ISO, CLAS consultant, Technical Security Architect) should be identified; Also, the Accreditor should formally sign off on the outputs of this stage.

6.2.9 If the RMADS has not yet been started it is beneficial to begin them at this stage (see Section 5). If the RMADS exists it is beneficial to update it according to include new information.

OGC Gateway 2 - IA requirements

6.2.10 The Accreditation process at OGC Gateway 2 (IS2 Stage 2 – IA Requirements) aims to produce an Information Assurance requirement for the tendering process of the project.

6.2.11 As part of any tender (ITT, Statement of requirement, or other equivalent tender document) the project/programme should provide a clear definition of the Information Assurance (IA) requirements. The requirements on the supplier for handling Protectively Marked material should be captured in a Security Aspects Letter. An IA professional should formally sign off on the tender document before they are issued to potential suppliers.

Inputs
• Inputs and Outputs of Stages 0 & 1; • IA Requirements derived from the risk assessment; • ITT/SoR or equivalent tender document.
Outputs (System and Accreditation Specific)
• IA requirements / Security Schedule • Revised Risk register to incorporate potential IA risks associated with tender. • Security Aspects Letter issued to the contractor

6.2.12 If the RMADS has not yet been started it is beneficial to begin them at this stage (see Section 5). If the RMADS exists it is beneficial to update it according to any changes to the information captured and the system itself.

OGC Gateway 3 – Investment Decision

6.2.13 The Accreditation process at OGC Gateway 3 (IS2 Stage 3 – Options Assessment and Selection) aims to assess a potential supplier’s capability and deliver a solution that meets the IA requirements.

Inputs
• Inputs and Outputs of Stages 0, 1 & 2; • Tender responses.
Outputs (System and Accreditation Specific)
• Revised risk register

6.2.14 During this stage an IA professional will need to be involved in the assessment of tender proposals to ensure that the suppliers have addressed the IA requirements in the tender documentation.

OGC Gateway 4 – Readiness for Service

6.2.15 The Accreditation process at OGC Gateway 4 (IS2 Stage 4 – Accreditation in Development and Acceptance) aims to confirm that the delivered solution is 'fit' for purpose in terms of the security requirements and is an 'accreditable' solution. It should be noted, that many of the activities and products contained in stage 4 & 5 provide the basis for re-accreditation of existing systems.

Inputs

- Products and security artefacts of Stages 0, 1 & 2;
- Updated Threat Assessment;
- Implications for new (or revised) legislation;
- Project, development & IA specific progress reports;
- Results of evaluation, verification and inspection activities;
- Configuration and change control information.

Outputs (System and Accreditation Specific)

- **RMADS**
- **IT Health Check Report**

  An IT Health Check Report (ITHC) is produced by a security testing company that is registered with CESG (see http://www.cesg.gov.uk/servicecatalogue/CHECK/Pages/index.aspx.
- **Pertinent Codes of Connection (CoCo's)**
- **Accreditation summary**
- **Accreditation decision**

6.2.16 During this stage the system should undertake an IT Health Check (ITHC) to assess the technical vulnerabilities of the technical components of the solution. In discussions with the Accreditor a remedial action plan may be required to address significant security issues.

6.2.17 As part of this stage the Accreditor will assess the RMADS as evidence that risks are being well managed. This may necessitate visits to site and/or the request of additional information. Once the Accreditor is satisfied as to the level of security he will produce an Accreditation certificate so that the system may go into live service. (The Accreditation certificate will have an expiry date, before which re-accreditation must be sought.)

6.2.18 When a system is accredited, with guidance from the Accreditor, the project/product manager will produce an Accreditation Summary to discuss the residual risks with the Information Asset Owner (IAO) of the system.

OGC Gateway 5 – Operations review and benefits realisation

6.2.19 The Accreditation process at OGC Gateway 5 (IS2 Stage 5 – Risk Management In-Service & Accreditation Maintenance) aims to ensure that the information system complies with its IA requirements and is being managed in accordance with the RMADS.

Inputs • Products from Stage 4; • Additional information on proposed changes • Incident reports; • Configuration and change control information; • RMDAS
Outputs (System and Accreditation Specific) • **Revised RMADS** • **New ITHC Report** • **Re-accreditation decision**

6.2.20 An independent annual review of the system to support re-accreditation should be carried out. The scope of the audit is at the discretion of the Accreditor (and may require an ITHC), who must ensure that the conditions for re-accreditation and accreditation review are clearly stated within the RMADS. A formal review of the Accreditation status of the system would automatically take place if any of the following events occur:

- Significant changes are made to the system;
- Significant changes to any risk component;
- The business use changes;
- The accreditation audit report or IT Health Check indicate significant concerns; or,
- A major security incident occurs.

6.2.21 As an output from this stage the Accreditor may produce an Accreditation audit report (in the case of a regular audit) and possibly a re-Accreditation certificate (in the case of a re-accreditation due to one of the possible reasons listed above).

System Decommissioning

6.2.22The Accreditation process at the closure of a system, or when a technical refresh of hardware, or when a hardware component fails and needs to be replaced (IS2 Stage 6 – Secure Decommissioning & Disposal) aims to ensure that when the system has reached its end of service life, the system/components are disposed of in a secure manner in accordance with National standards.

6.2.23The Accreditor will have oversight of the decommissioning and disposal process, with a final issue of a decommissioning certificate. The Accreditor should review the following for compliance with standards:

- Asset recovery;
- Contract closure;
- Removal of data from hardware, software, media etc;
- Secure disposal of storage media and solid state components used during the lifecycle of the system;
- Capture of audit logs in a readily accessible format;
- Decommissioning and disposal of the system/components; and,
- Security staff and user debriefing.

6.2.24The supplier will present the decommissioning certificate with identifying details of the hardware components being decommissioned, details of the method of sanitisation/destruction and the signature and details of staff conducting the work. The Accreditor and Security Manager will sign a Security Decommissioning Compliance Certificate that should be retained as a corporate record. This may be presented to the IAO/SIRO for information purposes.

7 Top IA Tips for a Successful Accreditation

This section highlights some tips that can be used as a checklist to de-risk the accreditation or re-accreditation of information systems.

What must the project deliver to the Accreditor?

1. Identify people to do the following roles: (so that roles are known in advance of any crisis) – see Section 3.
    - IAO – this should be someone at ACPO level; a risk decision maker who can escalate to the SIRO. The IAO may also be the Senior Responsible Officer.
    - IAO Advisor – the IAO can delegate day-to-day decisions relating to the risk management of the system, but cannot delegate risk.
    - Technical Security Architect – the TSA works for the project to ensure the proposed design meets security requirements
    - IA Advisor - works for the project offering procedural and other non-technical IA advice
    - RMADS author - usually but not necessarily CLAS, must be familiar with IS1&2 [ref 5 & 6], and must understand the need to be proportionate
    - Security Manager/ITSO - is typically required after the system is live, and acts as the initial contact for all security issues on the live service.
2. Set up a SWG and hold regular meetings - required to discuss security issues, manage security incidents and manage accreditation requirements
3. Hold Business Impact Level workshop - must agree BILs early on (and document the levels and their justification)
4. Privacy Impact Assessment or DPA compliance check (or argument for not requiring it)
5. Use the national police threat model for the threat assessment
6. Agree risk appetite (and tolerance if relevant)
7. Physical security assessments – covering sites such as data centres/terminal locations; the Accreditor may visit the sites
8. Agree vetting requirements (see National Policing vetting policy noting the distinction from HMG policy)
9. Create Security Operating Procedures (SyOps); users must be clear what is expected of them, and must sign their acceptance (regularly)
10. Establish cryptography requirements, if appropriate (the configuration may be checked during the CHECK ITHC)
11. Plan protective monitoring for the system
12. Gain technical assurance - use of assured products/solutions

13. Plan an ITHC - green light CHECK companies must be used. The SWG must agree scope, which must validate that countermeasures are in place and effective
14. Agreeing level of residual risk may need a workshop (this is not always a technical discussion)

What does the Accreditor need to accredit a new system?

1. Governance; evidence that proper governance is in place to ensure accountability for information and risks
2. Process; the required people in the right roles and all documentation supporting the risk management process
3. A risk assessment may be sufficient for an accreditation decision, but an RMADS is needed for full accreditation
4. Evidence-based RMADS; the content must be factual, not aspirational.
5. Expression of residual risk, which should be within the risk appetite of the service
6. Understanding by the business owner of the level of residual risk (at an appropriate level of seniority)
7. Escalated risk acceptance at the appropriate level (that is, by IAO/SIRO)
8. Documentation must include physical security assessments (meeting requirements) and statement of vetting (complying with policy)
9. ITHC must be done (to agreed scope)
10. Any significant issues raised by ITHC must be resolved
11. Remaining issues must be included in a remediation plan, which must be funded and have management commitment
12. Retesting should be built into the scope, or can be picked up the following year if the risks are sufficiently low.

What does an Accreditor need to re-accredit a system?

1. Governance must still be in place; if an SRO has moved on then an IAO must be named and aware of responsibilities
2. Evidence of ongoing security reviews, security incident management and active protective monitoring
3. RMADS must be reviewed (not necessarily re-written) - it must be updated in case of any changes, including threat levels
4. RMADS must still be factually accurate and the Accreditor will test some of its assertions
5. RMADS must include (updated) residual risk

6. Business owner must be aware of residual risk (at the appropriate level)
7. Physical security and vetting requirements must still be in place and reviewed.
8. Annual ITHC - by exception only, a conditional accreditation can be given if this is only planned but it must be committed and there can have been no significant change to the architecture or risk levels
9. Previous remediation plan must have been fully actioned. Current significant issues must have been resolved before a full accreditation can be given.
10. Remediation plan for remaining issues - as before, this should be funded and committed.

Control page

Distribution list

Recipient	Title	Location

Change control

Version	Date	Authority	Evidence of approval	Record of change
0.1	06 May 2009			Additional comments received for original document
0.2	12 May 2009			First stage comments received
0.3	20 May 2009			Review meeting comments received QRF 1 & 2
0.4	26 May 2009			Review comments QRF 3
0.5	09 June 2009			Review comments QRF 4
0.6	10 June 2009			Review of combined comments Accreditor and QRF forms
1.0	19 July 2009			Incorporation of Accreditation process flow model
1.1	22 July 2009			Insertion of second Accreditation flow graphic
1.2	7 August 2009			Re-write after broader community review.
2.0	1 Sept 2009			Re write of structure of document to improve readability.
2.2	10 Sept 2009			Minor modification to address comments of PIAAG
2.3	30 April 2010			Updates to encompass developments in Risk Appetite and Risk Balance, and to reflect changes to the IA Policy Framework
2.4	13 Dec 2011			Annual Document Review – Removal of IRO role, amendment from Risk Balance to Risk Escalation, Cross-references checked and minor reformatting.
2.5	19 Dec 2012			Annual Document Review (never published) – revision for changes to HMG standards
2.6	29 Nov 2013			Annual Document Review – update of references and revision of project manager guidance.

Page intentionally blank