Guidance for achieving Accreditation for new ICT Projects

Owner	NPIRMT
Author	Dave Jamieson, Helen Riccalton
Version	1.0
Date	17 January 2014

This document has been produced by NPIRMT.

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

Guidance for achieving Accreditation for new ICT Projects

Introduction

The following Tables identify key activities needed to achieve accreditation[1] of new ICT projects and services supporting, augmenting or replacing National Information Systems[2]. The aim of this paper is to assist Projects achieve accreditation for new ICT projects.

Pre-Contract Award

The following table identifies project activities which have Information Assurance/ Accreditation implications prior to award of a contract.

Requirement	Justification/Explanation
Brief National Accreditation Manager on new ICT service.	The Project Manager (PM) must brief the National Accreditation Manager on any new ICT project so a decision about the level of accreditation required can be estimated and an Accreditor[3] assigned.
Requirements Definition for new ICT projects.	Although for the business to determine, ensure the National Accreditor is involved in reviewing the security requirements for the service.
A Security Aspects Letter (SAL) for any potential suppliers may be required before contract award.	This ensures suppliers know how to transmit, store and dispose of any protectively marked material we will send them as part of the procurement exercise. This is produced by the PM in conjunction with procurement staff and the Accreditor.
A specific Security Schedule may be required as part of the contract for this service.	Procurement/commercial staff populate the document; and the PM ensures the Accreditor is involved in reviewing the security clauses for the service.
Agree scope of Accreditation (Development? Live? Test? Disaster Recovery? etc.)	This assists the PM understand the full scope of the system to be accredited,
Confirm vetting requirements	Ensure personnel security vetting requirements are agreed with the Accreditor and included in the contract, additional Police vetting[4] may be required, this may incur delays to the service if not identified early.
Information Assurance (IA) deliverables for project are identified.	These may include: • Business Impact Assessment; • Privacy Impact Assessment; • Technical Risk Assessment; • Risk Management & Accreditation Document Set (RMADS) this includes SyOPs; • Code of Connection; • Data Interchange Agreement; • IT Security Health Check (ITSHC) – CHECK Scheme; • Data Protection Compliance Check. Although identified by the Accreditor, these are project deliverables provided through Project Resource and the Project Manager must identify the people resource and cost necessary to deliver them within budget.

On Contract Award

Once a contract has been awarded the following activities need to be typically undertaken.

Requirement	Justification/Explanation
Suppliers may require a Security Aspects Letter (SAL) for this service	This ensures suppliers know how to transmit, store and dispose of any protectively marked material we will send them as part of the contract. This is produced by the Project Manager (PM) in conjunction with the Accreditor.
Review of supplier premises/data centre	To ensure that premises where Police Service data or code is developed, stored or processed are suitable. They need to be subject to a suitable audit regime. The PM should speak to the supplier and National Accreditor to establish what is required.
Identify stakeholders and	The PM needs to identify/resource the following functions:

resources to fill key appointments for the accreditation process	• Senior Responsible Officer (SRO); and/or • Information Asset Owner (IAO) usually the National Policing lead – this is normally a senior Police force representative. They are the business risk owner; • Information Asset Assistant (IAA), identified by IAO – day to day business decisions but risk ultimately remains with IAO; • Home Office/Project Technical Security Architect – to ensure proposed design meets IA requirements (not a supplier role); • IA Advisor – provides project with procedural and non technical IA advice (business resource/supplier, may be CLAS consultant); • RMADS Author –experienced in use of HMG Standards and ideally Police standards and policies, may be a CLAS consultant and could be provided by the supplier.
Set up Security Working Group (SWG)	Needs to involve business, supplier(s), project and Accreditor representatives. The project has to provide the secretariat function to support SWG meetings.

IA Deliverables & Significant IA Activities

This table gives additional guidance around the IA deliverables identified above.

Requirement	Justification/Explanation
Hold Business Impact Level (BIL) workshops	The key outcome is that the business confirms the BIL of the data. The system's security controls needed to protect the data are aligned with the BIL value. If the BIL is wrong then the security controls may need to be enhanced at a later date slowing the accreditation process and delaying the project.
Hold Privacy Impact Assessment workshops	This identifies any personal data issues that the system under development may involve. This may have a legal or regulatory impact on the project. This ties in with the Data Protection Compliance Check.
Agree risk appetite/risk tolerance of project	May involve SRO/IAO/Accreditor and the National SIRO. If not agreed can delay accreditation.
Agree if early IS1[5] technical risk assessment is required	Usually only for complex systems; this is to influence design of solution to ensure serious IA risks are identified and mitigated within the design, to preventing nugatory effort and costs.
RMADS[6] is produced	The RMADS author must talk to the Accreditor to ensure the structure, content and standards (e.g. values of National Information Threat Model[7]) to be used for the risk assessment, scope of accreditation, reliance scope, re-accreditation requirements etc is correct. This ensures the RMADS is delivered in line with the accreditation requirement.
Agree Cryptographic requirements	Whether HMG cryptographic products are required or commercial encryption is suitable. HMG cryptographic products have a long lead time and early engagement is necessary to ensure timely delivery.
Agree use of assured products/solutions and possible re-use of existing security services/solutions (e.g. IAM)	This may have significant cost savings for the project if they can reuse existing services.
Agree Protective Monitoring requirements/regime	This is a significant security control and needs to be built into the design of the service from the outset. Adding later always incurs significant additional costs. Some services will require little protective monitoring, others will require an extensive protective monitoring capability.
Plan ITSHC (CHECK Scheme)[8] regime	All new services must have an ITSHC before they can go live. Complex systems may require a number of ITSHCs before they can go live and an annual ITSHC is normally required.
Agree level of residual risk associated with solution	This may require a risk workshop with IAO and Accreditor to ensure the system will operate with residual risks that are within the risk appetite of the IAO.
Meet Code of Connection requirements	A Community Code of Connection[9] approval must be obtained before the system can connect to the national network

Develop and implement SyOPs for users	Users, whether normal users or privileged administrator users require clear guidance on acceptable behaviour with all national systems.

Achieving Accreditation

Once the above activities are completed, a review is undertaken by the Accreditor, looking for:

Requirement	Justification/Explanation
Governance is in place	IA roles have been filled and incumbents have accepted the IA responsibilities for the service and its data, includes the ongoing activities of the Security Working Group
Risk Assessment & Risk Treatment	A full accurate IS1 risk assessment has been completed identifying the known risks thus achieving a clear understanding of the level and type of risks. The risks have been reviewed; adequate risk mitigation strategies developed and implemented, sufficient evidence provided so that Accreditors have formal assurance that risks are treated with and the level of residual risk known. Where residual risks are outside of risk tolerance they must be escalated to the appropriate risk owner, IAO or National SIRO[10].
RMADS is complete.	It is factually correct, not aspirational, and covers all the areas above, and: • Residual risk to service is identified in business terms and within risk appetite – residual risk is owned appropriately (i.e. National Accreditor, IAO or SIRO); • Vetting requirements are identified and met; • Tailored IA controls specific to service are documented and implemented; • Baseline Control Set – showing technical, physical, personnel and procedural controls in place have been assessed to ensure they provide sufficient assurance to the business and identify any extant residual risks.
ITSHC (CHECK) has been completed.	All vulnerabilities are reviewed, context of the vulnerability provided along with existing mitigating controls. Critical, High and Medium risks need to be mitigated before go-live and all other risks managed through risk register and mitigated within 3 months of ITSHC report and where practical re-tested. An ITSHC remediation plan is required for extant (untreated risks) but may be included in the Risk Treatment Plan (below).
Extant Risks and issues.	Extant risks and issues that require action are included in a funded, resourced, Security Improvement Plan (Risk Treatment Plan) managed through the SWG.
Where relevant, a Data Protection Compliance Check has been completed.	Ensures the service is not in breach of any data protection legislation or regulatory requirements. Conducted by an experienced IA resource, though normally only required where personal data is being used for purposes other than which it was provided for.

Transition to Live Service	The PM needs to ensure service delivery management are aware of following:
	• The responsibilities of project SRO are transferred to the relevant business owner;
	• The SWG continues to meet,
	• Budget is identified for:
	  • ITHC plan for next year,
	  • Next iteration of RMADS
	• Patching policy commitment;
	• Protective monitoring review commitment.
	An Operational Security Manager needs to be identified and assigned to the service.

Contacts

Should you require any further information contact the Information Assurance mailbox (information.assurance@homeoffice.pnn.police.uk) with a subject line of FAO National Accreditation Manager.

Foot Notes

[1] Accreditation is a formal assessment of a system against its Information Assurance (IA) requirements, to ensure residual risks are acceptable to the business.
[2] For a definition of a National Information System see National Policing Accreditation Policy v2_0.doc
[3] Accreditors act as an impartial assessor of risk on behalf of the business.
[4] See www www.northants.police.uk/.../ac%5EACPO%20National%20Vetting%20Policy.pdf for details of Police vetting levels.
[5] IS1 is the standard risk assessment methodology used across Government. It is included in HMG Information Assurance Standard No1&2.
[6] Contents of RMADS etc is included in HMG Information Assurance Standard No1&2
[7] See National Policing Information Threat Model v1.2 dated 6 Nov 2013 for details of threats to Police ICT systems.
[8] See http://www.cesg.gov.uk/servicecatalogue/CHECK/Pages/WhatisCHECK.aspx for information on the CHECK scheme.
[9] Currently Community Code of Connection V3.3 dated April 2013.
[10] See ACPO/ACPOS Information Risk Appetite and Risk Escalation Case Guidance v1.2 dated 4 Jan 2012 for risk escalation process and risk ownership levels.