NICS

Information Assurance Policy

Version: 2.1

Reference: DF1/14/76211*

Author: Central IA Team

Approved by: Protective Marking Sub Group

Date: March 2014

Table of Contents

1. Document Information

Records NI TRIM Ref: DF1/14/76211*

1.1 Version History

Issue	Date	Description
1.0	May 2009	Information Assurance for Northern Ireland Civil Service
1.1	Sept 2011	NICS Information Assurance Policy
2.0	March 2013	NICS Information Assurance Policy V 2.0
2.1	March 2014	NICS IA Policy V 2.1 to reflect changes in Government Security Classification (April 2014)

1.2 Document Stakeholder List

Name	Role
Central IA Team	Editorial Control
NICS CIO	NICS IA Policy Owner
Protective Marking Sub Group	Approval

2. Executive Summary

2.1 Information Assurance (IA)

IA is the confidence that NICS information systems will protect the information they handle and will function, as they need to, when they need to, under the control of authorised users.

2.2 The NICS IA Policy Requirements

The policy requires departments to :-

- Provide a source of policy and guidance in line with the latest version of the Security Policy Framework (SPF) and place IA at the core of business processes.
- Ensure information assurance and management at the heart of customer and public services is as confidential, accurate and available as required.
- Place particular importance on the assessment and management of risks, clear accountability for such and ownership at Board Level. It includes a description of essential key roles for maintaining Information Assurance such as: Senior Information Risk Owner (SIRO), Information Asset Owner (IAO) and Accreditor.
- Provide a risk management approach to all IA related issues. It aids informed decision-making, bringing potential resource savings and efficiencies based on sound risk management practices which are pragmatic, appropriate, proportionate and cost effective.
- Be applicable to all information systems and services, including paper files, computers, communication systems and the information stored and processed on them as well as other NICS information assets.
- Recognise that the business needs of confidentiality, integrity and availability are integral parts of business delivery and public service, but that the individual impact of these may vary.
- Provide an IA risk management process that is continuous and lasts throughout the life-cycle of the information system by making accreditation or review a continuous process.
- Provide information risk management policy in support of shared services.
- Seek to ensure appropriate levels of professionalism, education and training.

3. Purpose and Objectives

3.1 Purpose

- To assist the NICS to meet its Legal and Regulatory obligations
- To support the NICS Information Security Strategic Aims and Objectives
- To support Information Asset Owners in discharging their roles and responsibilities

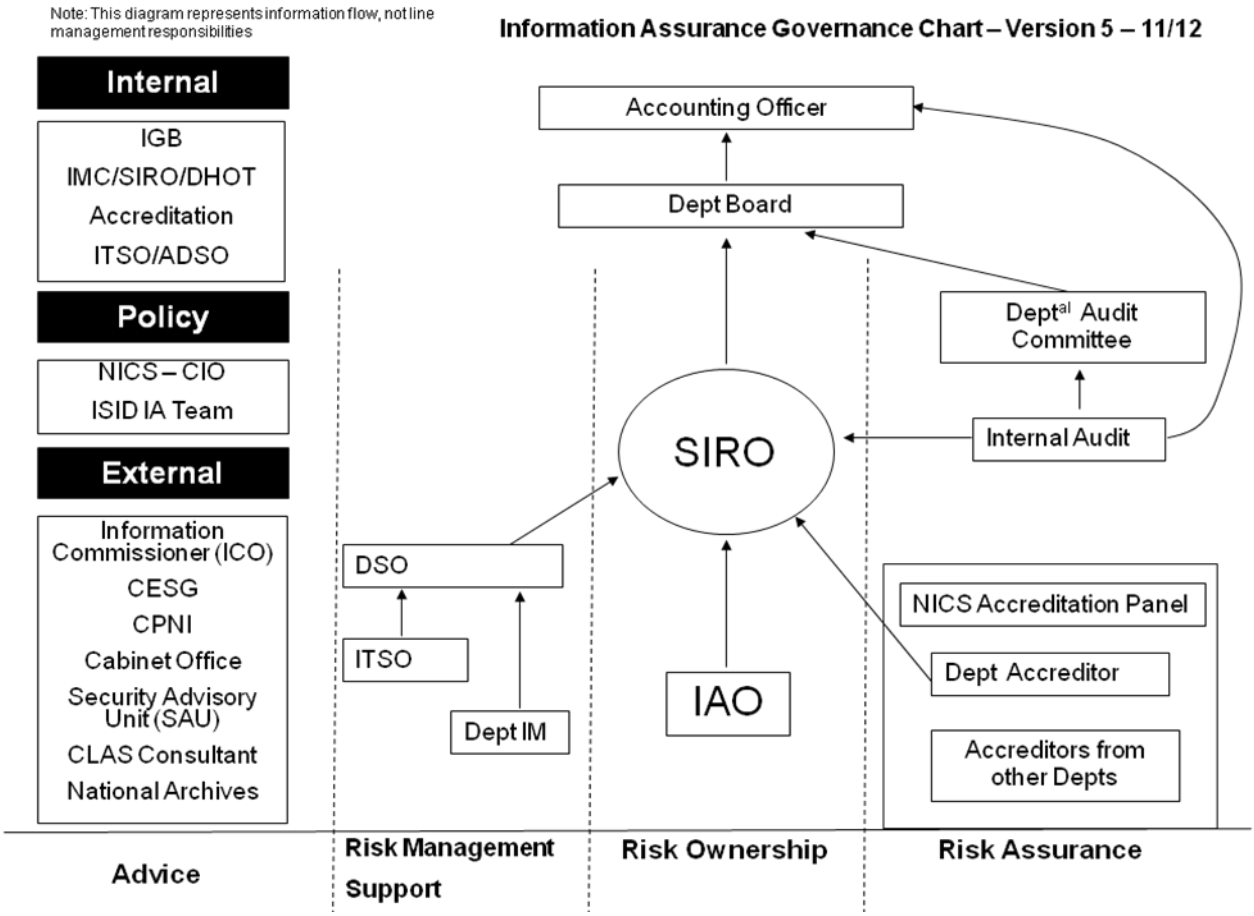
- To provide consistent implementation of IA standards across the NICS
- To enable greater consistency of Accreditation (inc. Shared Services)
- To assist the NICS to maintain connectivity with government organisations in GB.

3.2 Objectives

- Update the Information Assurance policy to align with current government IA policy, to ensure it is fit for purpose and relevant for the ICT landscape across the NICS;
- Explain the fundamental principles and requirements for information assurance;
- Promote understanding of Information Assurance as a business enabler and integral part of service delivery;
- Describe the existing arrangements and requirements for maintaining information assurance in NICS; and
- Highlight fundamental security requirements relevant to all staff in the NICS.

4. Governance

4.1 Information Assurance Governance Chart



4.1.1 Information Governance Board (IGB)

The Information Governance Board (IGB) provides the link between Information Assurance (IA), Information Management (IM) and ICT and gives strategic direction to the NICS.

4.1.2 NICS SIRO Forum

The NICS SIRO Forum is the primary decision making authority for Information Assurance within the NICS. The SIRO Forum makes strategic decisions and provides advice in a federated system where Departments manage under the direction of their own Minister and Boards but within a common structure which includes standards for IA, IM and ICT.

4.1.3 NICS Accreditation Panel

The NICS Accreditation Panel consists of representatives from across the NICS and makes accreditation decisions on matters of shared interest, such as: AccountNI; HRConnect; NetworkNI; ITAssist and RecordsNI. In addition, it provides a focal point for decisions affecting connections to publicly accessible

networks such as the Internet and the Public Services Network (PSN). As the sponsoring organisation, the NICS SIRO Forum acts as the approval authority and will take the final decision on any matter referred by the NICS Accreditation Panel – for such matters, the Panel will provide a recommended option.

4.1.4 NICS ITSO Forum

The NICS IT Security Officer Forum provides a means for representatives from across the NICS departments and wider public sector to discuss and share experience and guidance on aspects of Information Assurance and related matters of shared interest. It provides Information Assurance advice to the NICS Accreditation Panel for all applications, connections and networks within its remit. As the sponsoring organisation, the NICS Accreditation Panel acts as the approval authority and will take the final decision on any matter referred by the NICS ITSO Forum – for such matters, the ITSO Forum will provide a recommended option.

4.1.5 NICS Information Management Committee

The NICS IMC consists of Departmental Information Managers and provides a platform for NICS to collaborate, share best practice, consider appropriate policy development and make decisions to deal with new or challenging issues within the Information Management (IM) world. It provides the focal point for escalation, resolution and/or discussion for IM issues and considers implications for policy and training. Also, it liaises with the EDA Information Assurance Team, SIRO Forum and Departmental Heads of Technology and IT Assist to ensure that all relevant IM issues are covered.

4.1.6 Security Sub-Committees

It is recommended that each of the Shared Services should have a security sub-committee (similar to those for AccountNI and NetworkNI). The sub-committees' Terms of Reference will include the provision of continuous assurance to the IA Fora that IA activities are being conducted to secure the system/service to the appropriate level of its IA requirements in the context of its business needs.

4.1.7 Central IA Team

The Central IA Team provides administrative support to each of the IA Fora and the NICS Accreditation Panel, as well as advice and guidance on IA policies and standards across the NICS. It also takes the lead on the provision of assurance to Head of Civil Service on the efficiency and effectiveness of the protective regime on an annual basis in the form of the Security Risk Management Overview (SRMO).

Email: isid.iateam@dfpni.gov.uk

4.2 Roles and Responsibilities

4.2.1 Senior Information Risk Owner (SIRO)[1]

The SIRO is familiar with information risks and leads the Department's response. The SIRO is the focus for the management of information risk at Board level and represents the Department at the NICS SIRO Forum.

[1] Role mandated by the SPF.

4.2.2 Information Asset Owner (IAO)[1]

The IAO understands and addresses risks to the information, both electronic and paper based, in their business area and provides assurance to the SIRO's information risk assessment.

4.2.3 Departmental Security Officer (DSO)[1]

The DSO has day-to-day responsibility for all aspects of Protective Security, (Physical, Information and Personnel).

4.2.4 Departmental Accreditor

The Accreditor is responsible for the accreditation of all systems that operate in the Department and represents the Department on the NICS Accreditation Panel.

4.2.5 Departmental IT Security Officer (ITSO)

The ITSO supports the Departmental Security Officer (DSO) on all IT Security matters and represents the Department at the NICS ITSO Forum.

4.2.6 Departmental Information Manager (DIM)

The DIM provides support and advice to the SIRO, IAOs and Business Area Information Managers.

4.2.7 Crypto Custodian and Deputy

The crypto (deputy) custodian, in line with HMG IA Standard No. 4, manages the cryptographic account for CESG-approved material, such as that used for NICS encrypted laptops and ironkeys. The DOJ has a separate cryptographic account.

4.2.8 Security Advisory Unit (SAU)

The Security Advisory Unit (SAU) is part of OFMDFM. Key responsibilities include receipt and dissemination of protective security and terrorist threat information, physical security surveys and audits, advice to departments regarding security provisions in contracts. **The security vetting policy advisory function has transferred to Appointments and Marketing Branch, DFP.**

4.2.9 Senior Responsible Owner (SRO)

SROs are responsible for ensuring security is catered for in their projects and dealt with by design, including resulting contracts. To this end, a Privacy Impact Assessment is required for all new projects as well as the application of IA standards

4.2.10 Further Details

Further details of these roles and responsibilities can be found in **Appendix A**

5. Accreditation and Risk Management

5.1 Introduction

The Accounting Officer/Permanent Secretary in each Department is responsible for the IA governance within their Department. Governance arrangements in the NICS are centred on Departments being responsible for the risk management and accreditation of their line of business information systems and services.

It should be borne in mind that paper file stores of sensitive information, whilst not requiring accreditation, do require information assurance and risk management and should be reviewed periodically.

The accreditation of ICT systems or services handling, storing or processing personal or sensitive information or business critical data is a formal, independent assessment against its IA requirements, which results in the acceptance of residual risk in the context of the business requirements and information risk appetite. This is a prerequisite for approval to operate.

The current default NICS risk appetite is "cautious" and is under review. For details on risk appetite, see: Good Practice Guide (GPG) 47, Information Risk Management[2].

5.2 Description

A fundamental principle of information risk management is technical risk assessment. Departments must conduct a technical risk assessment and risk treatment for the Confidentiality, Integrity and Availability of their ICT systems and services. The risk management must follow HMG IA Standards. It must include a business impact and threat assessment. **It is important to note that the Departmental Board will still own the risks to their information even where their services have been outsourced [see paragraph 6.1] or are part of a shared service.**

The accreditation and risk management process must be compliant with all legal and regulatory obligations as well as all HMG Standards and Good Practice Guides (GPGs) and GPG No. 47, Information Risk Management

IS1&2 allows Departments to establish their own requirements for accreditation whilst taking into account the wider business context. This proportionality is critical for cost savings and business objectives to be realised.

The process will require a Risk Management & Accreditation Document Set (RMADS) or an IA compliance statement. These deliverables should be proportionate and appropriate to the level of complexity and risk to the system or service being accredited.

The Business Impact Level (BIL) will be a significant factor in determining the complexity of the RMADS.

There is no reason why simple systems cannot have a short and basic RMADS. However, it is essential that the rationale behind this decision be documented.

5.2.1 Security Operating Procedures (SyOPs)

SyOPs must be produced for all users or providers of ICT systems and services. Users or providers must acknowledge that they understand the content of the SyOPs and that they will follow the procedures. This is a useful means of providing traceability and accountability.

[2] To access IA Standards and GPGs, it will be necessary to register with the CESG website. Do so at: http://cesgiap.gsi.gov.uk/index.php and register your email address in the format : firstname.lastname@deptni.gsi.gov.uk.

5.2.2 Re-accreditation and Review

- The NICS accreditation period will normally range from three to five years, depending on the IA profile and complexity of the system.
- The accreditation period for Enterprise Shared Services (ESS) will not exceed three years.
- All accreditation should be reviewed at intervals not greater than 18 months.

5.2.3 CLAS Consultancy

- CLAS, the CESG Listed Advisor Scheme, provides a pool of private sector providers approved by CESG to provide IA advice to Departments.
- The use of external advice to support the accreditation process should be proportionate and considered. External providers should only be brought in to support areas of significant challenge and where additional independent resource is required.
- Further details in relation to negotiated contracts available from CPD.

5.2.4 IT Health Check (ITHC or CHECK)

- This is an independent technical analysis of a system or service to ensure correct implementation of security functions and the identification of vulnerabilities which may compromise the Confidentiality, Integrity or Availability of information.
- An ITHC must be conducted on an annual basis for systems or services which are:
    - Enterprise Shared Services or,
    - Public-facing, on the Internet or,
    - Business Critical or,
    - The IA profile is assessed as high risk.
- An ITHC should be considered on an annual basis and conducted at intervals no greater than 18 months as part of the accreditation review process. The results will determine whether or not further information risk management activities will be needed including re-accreditation.

5.2.5 Call-Off Contracts

Two call-off contracts have been prepared by Central Procurement Division (CPD) for the purposes of procuring CLAS and CHECK services. They are relevant for contracts above and below the European financial threshold. Departments are encouraged to tailor them to their own needs.

5.2.6 Secure Disposal and Sanitisation of Media and Equipment

When information is no longer required, Departments' IAOs must ensure that all media used for storing and processing protectively marked or otherwise sensitive information must be sanitised and, if necessary, disposed of in accordance with HMG IA Standard No.5 Secure Sanitisation A call-off contract for this purpose exists in CPD.

5.2.7 Business Continuity Planning

- All information systems should have a Business Continuity Management process to counteract interruptions to business activities and protect business critical processes from the effects of major failures or disasters. Contingency and disaster recovery plans for the technical infrastructures and key accommodation must be aligned with this process.
- As part of the annual accreditation review process, the system owners/security managers should provide assurance that Business Continuity and ICT Contingency Plans have been reviewed and tested.

5.3 Proportionate Approach to Accreditation

5.3.1 Description and Purpose

It has been agreed that the type of systems which will be suitable for this approach will match each of **eight** criteria and will include simple word, database or spreadsheet based systems developed locally within Departmental ICT Services and stored outside the scope of NICS or Departmental accredited systems.

This approach is appropriate for systems **with no external connections** either for maintenance or user access and which process and store personal and sensitive material with a Business Impact Level (BIL) of no greater than Impact Level (IL2) for Confidentiality, Integrity or Availability. For guidance on BILs see: Appendix B of HMG IA Standard Nos. 1&2 Supplement Technical Risk Assessment and Risk Treatment

Systems which contain Personal Information must be handled in accordance with the Cabinet Office's Security Policy Framework (SPF).

Where systems do not match all of the eight criteria, this approach should **not** be used. Instead, the principles described in paragraph 5.2 above must be applied.

For details, see : NICS Generic Approach to Risk Management and Accreditation

The same approach has been approved for systems which exactly match the same eight criteria and have a BIL of no greater than IL3 for C, I and A.

For details, see : NICS Proportionate Approach to Risk Management and Accreditation IL3

6. Assuring Connections to the NICS Infrastructure

6.1 Introduction

As the risk to an organisation's information assets cannot be transferred to a supplier or sub-contractor, visibility of the supply chain is of paramount importance. Therefore, any requirement concerning the protection of information assets by a supplier should be explicitly referenced in the contract, including any limitations concerning supply chains (e.g. restricting the use of re-sellers etc), offshoring, shared services or further outsourcing. HMG GPG No.6, Outsourcing & Offshoring – Managing the Security Risks

From the procurement stage, Departments must ensure that the security, procurement and contract management teams work together to ensure that adequate security, information assurance and business continuity arrangements are specified in contracts with third party suppliers. Central Procurement Division (CPD) will provide Schedule 6 to assist in this.

Departments may decide that aspects of their own IA policies are suitable to be used as the basis for contract creation or legally binding agreements. Where this is the case, business and security requirements need to be clearly communicated to those with contractual responsibility so that they are understood and incorporated into contracts or legally binding agreements. Departments should, in the first instance, contact their commercial and legal teams, as well as Central Procurement Division.

In all cases, the Registration / Onboarding processes and Through-life assurance processes referenced at paragraphs 6.3 and 6.4 must be followed.

6.2 Use of the Baseline Control Set (ISO 27001 Controls)

ICT Services and Systems connecting to NetworkNI at IL3 and above for Confidentiality, Integrity or Availability must, as a minimum, implement the full set of controls as defined in the Baseline Control Set which can be found in Appendix A of HMG IA Standard Nos. 1&2 Supplement Technical Risk Assessment and Risk Treatment

ICT Services and Systems connecting to NetworkNI at IL2 and below for Confidentiality, Integrity or Availability must select pragmatic and appropriate controls from the Baseline Control Set which can be found in Appendix A of HMG IA Standard Nos. 1&2 Supplement Technical Risk Assessment and Risk Treatment

6.3 Registration Requirements for Systems Connecting to NICS

Registration Requirements for Systems Connecting to NICS : TRIM Ref DF1/12/324097* MUST be completed for all systems connecting to NICS.

6.4 NICS Online

The NICS Online IA Framework has been developed to ensure a high level of Information Assurance for the NICS. It represents good practice in relation to Information Assurance and the principles henceforth must be applied to all NICS websites. Those websites and/or applications which are citizen-facing must use the NI Direct Online Information Assurance Framework [Trim Record Ref: DF1/11/352879*]

NICS Online Information Assurance Framework

7. Training and Professionalisation

7.1 Information Assurance Roles

All staff with specific roles in Information Assurance must attend the courses needed to achieve and maintain competencies and skills, and these staff are encouraged to obtain relevant professional qualifications.

Information on training courses and professionalisation can be found on the CESG website.

Details of roles, responsibilities and training can be found in **Appendix A**

8. Incident Response and Forensic Readiness

8.1 Information Security Incident Policy

Departments must have clear, tailored policies and procedures for reporting, managing and resolving information security breaches and ICT security incidents. Generally, the first call should be to the DSO/ADSO or ITSO and ITAssist who will invoke the appropriate procedures.

For details, see: IT Assist Information Security Incident Reporting Policy [Trim Record Ref: DF1/11/290364*] and the NICS IA Framework.

8.2 Forensic Readiness Policy

Departments must have a forensic readiness policy that will maximise the ability to preserve and analyse data generated by an ICT system that may be required for legal and management purposes. Generally, the first call should be to the ITSO and ITAssist who will invoke the appropriate procedures.

For details, see: IT Assist Forensic Investigation of ICT Equipment [Trim Record Ref: DF1/11/353909*] and NICS Forensic Readiness Guidelines.

There should be an annual exercise of the Incident Response Procedures and Forensic Readiness Plan.

9. Information Asset Registers

IARs must contain details of the accreditation status of all ICT systems holding sensitive or personal information. Likewise, they should hold review details of file registers and paper stores where protectively marked information appears (see NICS IAO Handbook).

10. Other NICS IA Policies

Information Assurance is an enterprise-wide activity. Consequently, some policies overlap and responsibilities fall under the remit of different areas. The IA policies will be reviewed regularly with a view to reducing their number. The three websites where most IA policies can be found are :

Central IA Team

Enterprise Shared Services

HR Connect

NICS IA Policies are issued by the NICS CIO following a development and approval process which includes the NICS SIRO Forum, the NICS Accreditation Panel and the NICS ITSO Forum. The policies outline the minimum measures that should be implemented. Central IA Team welcomes feedback and encourages readers to comment at isid.iateam@dfpni.gov.uk

A list of other relevant policies is available at Appendix B.

11. Appendix A

11.1 Roles, Responsibilities and Training (as defined in HMG GPG 47)

11.1.1 Senior Information Risk Owner (SIRO)

- Should attend an Information Risk Management course.

  Details of courses can be found at the National Archives website.
- Is a member of Management Board who takes ownership of information risk
- Leads and fosters a culture that values, protects and uses information for the public good
- Owns the overall information risk policy and risk assessment process, tests its outcome, and ensures it is used
- Ensures that the Departmental Risk Register is up-to-date
- Advises the Accounting Officer on the information risk aspects of the Statement on Internal Control
- Signs the Security Risk Management Overview (SRMO) for Head of Civil Service (HOCS)

11.1.2 Information Asset Owner (IAO)

- Is recommended to attend an Information Risk Management course.

  Details of courses can be found at the National Archives website.
- Is recommended to be a Grade 7 (or Higher) within the business area
- Fosters a culture that values, protects and uses information for the public good
- Knows what information the asset holds (Information Asset Register) and what enters and leaves it and why
- Knows who has access and why, and ensures their use of it is monitored
- Understands and addresses risks to the asset, and provides assurance to the SIRO
- Ensures the asset is fully used for the public good, including responding to requests for access from others

11.1.3 Departmental Security Officer (DSO)

- Departments must ensure that DSOs have either attended relevant training courses before or, at the earliest opportunity, after appointment
- Day to day responsibility for all aspects of Protective Security including physical, personnel and information security
- Implementation and dissemination of protective security policy
- Decisions on personnel security matters
- Guidance for incident reporting

- Education and training

11.1.4 Departmental Accreditor

- All accreditors must attend at least a one day overview of the accreditation process. In addition, anyone involved in accreditation reviews on behalf of their accreditor must attend the relevant courses.
- Responsible for the accreditation of line of business systems that operate in the department and provide statement recording same
- Makes decisions on further actions needed e.g. timing and scoping of Health Checks etc
- Provides direction on frequency of security reviews – normally annually depending on nature of business
- Represents the department on the NICS Accreditation Panel
- Oversees the accreditation process within department

11.1.5 Departmental IT Security Officer (ITSO)

- Departments must ensure that ITSOs have either attended relevant training courses before or, at the earliest opportunity, after appointment
- Advises Accreditor on the accreditation of information systems
- Records the accreditation status of information systems
- Ensures that Accreditor is involved in new systems from the concept stage onwards
- Advises Accreditor of any planned changes to systems
- Provides advice and guidance to departmental staff regarding the accreditation process within department
- Acts as Incident Response Handler in the event of a major incident affecting information systems in the department
- Provides advice and guidance to department and agencies to ensure they are compliant with IA policy
- Attends / represents departmental interests at ITSO forum and ensures good practice
- Assists with information assurance awareness for all staff
- Reports to the Departmental Security Officer (DSO) on ICT security matters

11.1.6 Departmental Information Manager (DIM)

- Ensures that relevant FOI and DPA policies and guidance are in place, updated when necessary and approved by the Departmental Board.
- Ensures regular reports are provided to Departmental Board.
- Implements and monitors departmental policy in relation to information management.
- Assists with the establishment and maintenance of an Information Asset Register.
- Provides central point of contact for other areas of information management expertise e.g. libraries, registries.

- Ensures regular information audits are undertaken for department and produces and addresses reports on outcomes of documentation as necessary.
- Liaises with Departmental Board to ensure that information management is incorporated into business planning.
- Ensures the role of Business Area Information Managers and responsibilities of IMU/IMB are reviewed in conjunction with current information management projects and strategies.

11.1.7 Crypto Custodian and Deputy

- Responsible for ensuring that all CESG cryptographic products e.g. Brent keys, Bitlocker Key Material, AEP Key Material, are ordered, managed, stored and destroyed in accordance with HMG IA Standard No 4. Management of Cryptographic Systems
- Custodians and their Deputies must attend the Custodian Course approved by CESG.

11.1.8 All Staff

- All staff must undertake the NICS Online Training Package in all topics available. This will form part of the induction programme for all new entrants. Staff with privileged accounts or who manage/support information systems require additional training.
- All IA specialists are encouraged to pursue CESG Certification for IA Specialists.

12. Appendix B

12.1 NICS Laptop and Mobile Device Security Policy

In the event of the loss or theft of an encrypted NICS Laptop or Ironkey, the user must ensure that their Line Manager, ITSO and IT Assist are informed as soon as possible. [Trim Ref: DF1/14/68915]

12.2 NICS Clear Desk Policy

12.3 HR Handbook Section 6.11 Use of Electronic Communications

12.4 Guide to Document and IT Security

12.5 Ten Key Rules

13. Glossary

Term/Abbreviation	Meaning
AccountNI	NICS Financial Services delivery partner
Accreditation	A formal, independent assessment of an ICT system or service against its IA requirements in the context of business need
ADSO	Assistant Departmental Security Officer
Baseline Control Set	Set of protective controls to manage information risk
BIL	Business Impact Level
Business Continuity	Activity performed to ensure business critical functions will be available
CESG	Communications-Electronic Security Group
CIO	Chief Information Officer
CLAS	CESG Listed Advisor Scheme
DSO	Departmental Security Officer
EDA	Enterprise Design Authority
ESS	Enterprise Shared Services
Forensic Readiness	Ability to collect credible digital evidence
GPG	Good Practice Guide
HRConnect	NICS Human Resources delivery partner
Information Asset	A body of information, defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycles.
IAO	Information Asset Owner

Term/Abbreviation	Meaning
IM	Information Management
Ironkeys	ITAssist issued USB approved for data transfer and storage
IS1/IS2	HMG IA Standards No.s 1 and 2
ISO/IEC 27001	The international Standard and Guidelines providing a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System.
ITAssist	NICS ICT Services delivery partner
ITHC	IT Health Check
ITSO	IT Security Officer
Line of business	Services provided by a particular Department
NetworkNI	NICS ICT Infrastructure delivery partner
NICS	NI Civil Service [All Departments, NDPBs, ALBs etc]
NI Direct	NI Government services delivered online
Offshoring	Relocation by an organisation of a business process from one country to another
PSN	Public Services Network
RecordsNI	NICS Electronic Document Records Management System
Risk Appetite	The level of risk that an organisation is prepared to accept
RMADS	Risk Management Accreditation Document Set
SIRO	Senior Information Risk Owner
SPF	Security Policy Framework
SyOPs	Security Operating Procedures
TRIM	Tower Records Information Management used for RecordsNI

14. References

1. HMG Security Policy Framework, v11.0
2. HMG Information Assurance Standard 1&2 Information Risk Management
3. HMG Information Assurance Standard 1&2 Technical Risk Assessment and Risk Treatment
4. HMG Good Practice Guide No. 47, Information Risk Management
5. HMG Good Practice Guide No. 6, Outsourcing and Offshoring – Managing the Security Risks
6. HMG Information Assurance Standard No. 4, Management of Cryptographic Systems
7. HMG Information Assurance Standard No. 5, Secure Sanitisation
8. NICS Generic Approach to Risk Management and Accreditation TRIM Ref: DF1/12/97540*
9. ISO/IEC 27001 Information Technology Security Techniques, Information Security Management Systems — Requirements
10. Registration Requirements for Systems Connecting to NICS : TRIM Ref DF1/12/324097*
11. NICS Online IA Framework, http://online.nigov.net
12. NI Direct Online Information Assurance Framework : TRIM Ref: DF1/11/352879*
13. IT Assist Information Security Incident Reporting Policy : TRIM Ref: DF1/11/179398*
14. IT Assist Forensic Investigation of ICT Equipment : TRIM Ref: DF1/11/353909*