

NATIONAL RECORDS OF SCOTLAND

preserving the past; recording the present; informing the future



2011 Census

Information Assurance Policy Statement By the UK Census Offices

June 2011

NATIONAL RECORDS OF SCOTLAND joins together



General Register Office
for
SCOTLAND

information about Scotland's people



THE NATIONAL
ARCHIVES OF SCOTLAND

Table of Contents

1. Introduction	3
2. Information classification.....	4
3. Information risk management.....	5
4. Governance	6
5. Accreditation	6

1. Introduction

- 1.1. This document outlines the policy and commitments that the three UK Census Offices for England and Wales (The Office for National Statistics (ONS), Scotland (The National Records of Scotland (NRS) and Northern Ireland (The Northern Ireland Statistics and Research Agency (NISRA)) are adopting on Information Assurance (IA) for the 2011 Census.
- 1.2. The UK Census Offices have reached joint working agreements on some key aspects of IA with the aim of providing a consistent approach across the UK. There are also some differences between the approach adopted by each Census Office which reflects local business requirements and operational arrangements.
- 1.3. The policy statement gives joint commitments and aims to preserve:
 - the confidentiality of information by ensuring it is only available to those who are authorised to access it;
 - the integrity of information by safeguarding the accuracy and completeness of information; and,
 - the availability of information by ensuring that users have access to information and information systems as and when required.
- 1.4. The policy also intends to ensure compliance with the HMG Security Policy Framework (SPF)¹.
- 1.5. What is information assurance?
 - 1.5.1. Information assurance is defined in HMG IA Standard No. 2 – Risk Management and Accreditation of Information Systems [Issue 3.2 January 2010] as ‘the confidence that information systems (and services) will protect the information they handle and will function as they need to, when they need to, under the control of legitimate users.’
- 1.6. Why is information assurance important?
 - 1.6.1. Census data is a critical asset for the development of Government policy and for allocation and targeting of resources.
 - 1.6.2. The UK Census Offices must have confidence that data collected, stored, processed, analysed and output by the three UK Censuses is fit for purpose and meets user needs. It must also meet the public undertakings given that Census data will be kept in the strictest confidence and will be used solely for the production of statistics.

¹ See http://www.cabinetoffice.gov.uk/sites/default/files/resources/hmg-security-policy_0.pdf for Security Policy Framework

2. Information classification

- 2.1. The Government Protective Marking System (GPMS) is the system used by the UK Government and the UK devolved administrations to ensure that access to information and other assets is correctly managed and safeguarded. The system is designed to support business and meet the requirements of relevant legislation, international standards and international agreements.
- 2.2. The UK Censuses count everyone in the UK once every 10 years. They are the biggest and most complex statistics gathering exercises in the UK. The Censuses employ large temporary field forces to manage the delivery and collection of over 30 million questionnaires to the public. During the different stages of the Census operations information about individuals and households is held electronically in databases, on digital images, on microfilm and on paper. Census information is given to each of the Census Offices by the public in the strictest confidence and on the understanding that it will only be used for the production of statistics. There are legal penalties for the unlawful disclosure of personal Census information by anyone involved in a Census operation.
- 2.3. The sheer scale and complexity of the UK Censuses make it difficult to apply a single protective marking for all Census information about individuals and households. However, the Census Offices recognise that the standards and procedures appropriate for RESTRICTED level operations provide a suitable baseline for security solutions required to manage Census information.

3. Information risk management

- 3.1. Risk management is an iterative process that is carried out throughout the lifecycle of the UK Censuses. The Census Offices have adopted a risk management approach to cover all areas of protective security². The assessment of risk is carried out using HMG standards and the outcome is documented in a Risk Management Accreditation Document Set (RMADS).
- 3.2. The level of impact likely to result from any compromise of confidentiality, integrity and availability of information is assessed using Business Impact Level (BIL) tables in HMG IA Standard No. 1 – Technical Risk Assessment³. The tables use a seven point scale to enable the Census Offices to make a balanced assessment of the countermeasures needed to meet requirements.
- 3.3. The BIL tables A4 (Public Services) and A6 (Public/Citizen) most closely relate to the business of the UK Censuses. However, the BIL tables for all business areas and sub-categories were assessed for completeness and to ensure that the process did not identify any issues that needed consideration. The maximum BIL for the UK Censuses is 4.
- 3.4. Each of the Census Offices has set an overall level of risk that they are prepared to tolerate to achieve their business aims.
- 3.5. The Census Offices are risk averse and are prepared to tolerate a low level of risk in all areas of the business.
- 3.6. Information systems that hold Census information about individuals and must go through a formal accreditation process to ensure compliance with HMG IA Standard No. 2.

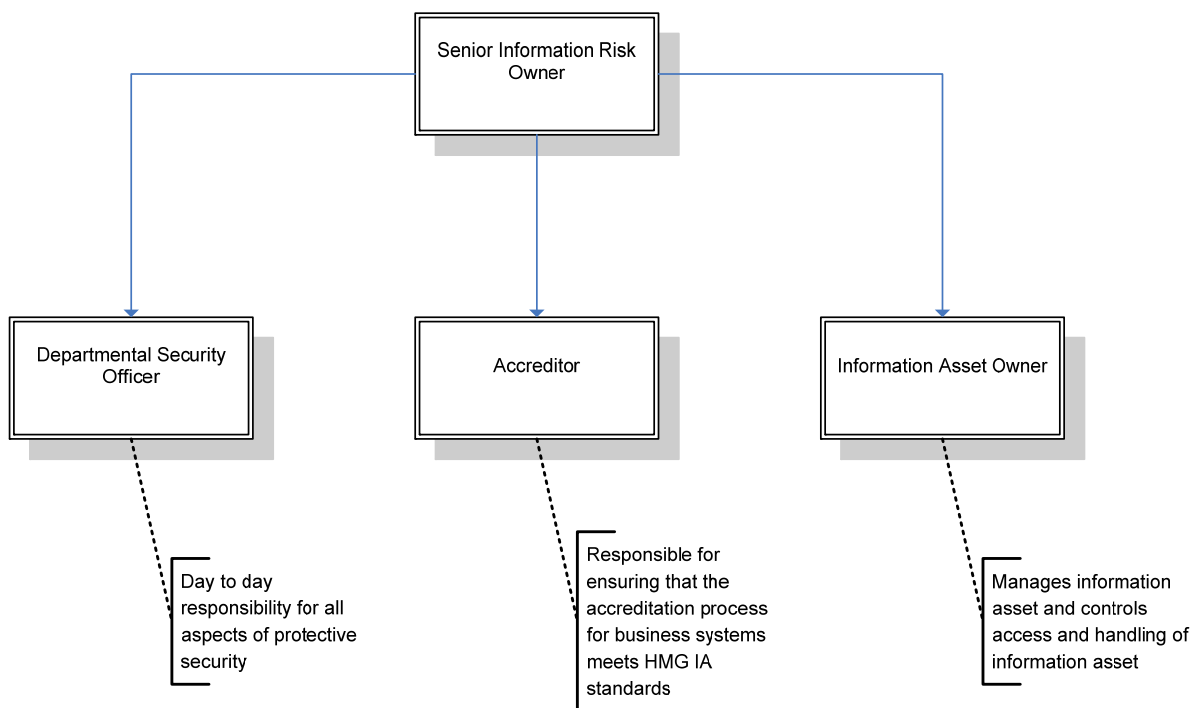
² Physical, personnel, procedural and information security.

³ See http://www.cesg.gov.uk/policy_technologies/policy/media/business_impact_tables.pdf for BIL tables.

4. Governance

- 4.1. The Census Offices have established governance arrangements to manage information assurance. Within each Office a Senior Information Risk Owner (SIRO) is responsible for Census information risks. The SIRO ensures that appropriate arrangements are in place for the effective delivery of information assurance. The SIRO is supported by other roles including an Accreditor, Information Asset Owners and the Departmental Security Officer.
- 4.2. The Census Offices have also set up a UK Census Information Assurance Working Group (UK CIA WG) to promote a common strategy and deal with overarching Census IA issues. This group has representatives from each Census Office.
- 4.3. The governance arrangements and the main roles in each Census Office are shown in Figure 1 below.

Figure 1



5. Accreditation

- 5.1. The formal assessment of an information system against its Information Assurance requirements, is called Accreditation. This assessment may result in the acceptance of risks that cannot be mitigated (called residual risks) without adversely impacting the business itself. It is government policy that if a system contains protectively marked information, or is part of the Critical National Infrastructure (CNI) it should be subject to Accreditation.

- 5.2. Any business activity involves risk, to the organisation, to other business activities, to clients, customers and partners. Some of these risks are security related, in that they involve threats to the confidentiality, security, integrity and availability of its information and business processes, or to the ability of the organisation to monitor its own activities and comply with the law. Accreditation is the process whereby these risks are assessed, and cost-effective countermeasures are determined and put in place. It includes the point at which the residual risks are formally accepted on behalf of the organisation.
- 5.3. Accreditation is fundamental to the assurance and delivery of any 'trusted' system or service that underpins government business. It is a continuous process, throughout and beyond the life of the delivery project. All Census systems will be subjected to the accreditation process.