Scotland's
Census 2011
Shaping our future

2009 Census Rehearsal Evaluation
Security

January 2010

Table of contents

2009 Rehearsal – Security

1. Introduction

1.1 The General Register Office for Scotland (GROS) must provide assurance to members of the public, other census stakeholders and Government ministers regarding our commitment to maintaining the confidentiality and security of the personal information collected during the census operation. The 2009 rehearsal allowed us to test our security measures and identified valuable lessons regarding improvements that can be considered for implementation for the 2011 Census programme.

1.2 This paper encompasses all census areas that have been security assessed during the rehearsal.

2. Evaluation Objective

2.1 The objective of the evaluation process was to:

- review the effectiveness of security measures adopted during the rehearsal;
- provide assurance of contractor compliance against agreed security controls; and
- allow for security recommendations and improvements to be considered for implementation for the 2011 Census.

3. Evaluation scope

The scope of the evaluation process covered all areas of the census, both the in-house service provision and the services provide by the main census contractor.

3.1 The areas covered within this report include:

3.1.1 In-house operations:

- Census Fieldwork operations and GROS in-house services (including the helpline, a variety of supporting Information Communication Technology (ICT) systems, security awareness training and incident management).

3.1.2 Out-sourced operations:

- print;
- internet services;
- Paper Data Capture (PDC); and
- logistics.

4. Government Security Standards

4.1 The rehearsal security evaluation process was assessed against the mandatory requirements of the HMG Security Policy Framework. This was also supported by compliance with the following UK Government Communications-Electronics Security Group (CESG) Information Assurance Standards:

Standard No 1; Standard No 2; Standard No 4; Standard No 5; and Standard No 6.

4.2 In addition to the above government standards, the rehearsal was assessed against International Security Standard (ISO 27001) and the 2011 Census Confidentiality Declaration and Guidelines. All internet services are compliant with eGovernment Security Assurance Framework (eGSAF).

4.3 Our main contractor worked closely with a third party security organisation to provide an independent review of their performance set against contractual obligations.

5. Management of GROS Census Security

5.1 GROS has an established Security Team who have years of experience working within the information security specialism. This team provides day-to-day guidance and direction to GROS management and staff on the most appropriate security measures for GROS business.

5.2 A new dedicated Census Security Team (CST) has been established, drawn from members of staff working within the information security arena and census business operations areas. The focus of the new CST is to ensure the confidentiality, integrity and availability of the census operation, to provide assurance, guidance and direction on the most effective security arrangements appropriate for the census business process.

5.3 During the rehearsal, security provision was integrated into each operational area.

5.4 For 2011, an advisory and assurance group, the Census Security Assurance Group (CSAG) has been established including representatives from all areas of the census operation, for both in-house and out-sourced services. This group oversees and monitors the provision of all security across the whole programme at a strategic level. This group ensures that program-wide information security controls fit within the census security strategy and the GROS census confidentiality requirements.

5.5 Risk Management & Accreditation Documents Sets (RMADS) were produced by the main census contractor for the out-sourced services, Print, Internet and Paper Data Capture. These are portfolios of security documentation, which include full risk assessments of the service and its IT systems including the roles and responsibilities of the staff involved, as well as a risk register, a risk treatment plan plus full system security operating instructions for the contracted out services. The RMADS comply with HMG Information Standards and the ISO 27001 international standard. Full audit and compliance checking of the RMADS will be continued throughout the 2011 Census operation.

6. Field Operations

6.1 All census field staff were subject to the same terms and condition of employment as that of established civil servants and were therefore subject to the same Civil Service privacy obligations.

6.2 Background checks for field staff were much more robust for 2009 than for any previous census. As part of the rehearsal employment process, all census field staff underwent pre-screening employment security checks as part of the recruitment process and completed security awareness training which defines their obligations in holding, storing and restricting access to the census information in their care. In addition, all field staff signed the Census Confidentiality Undertaking (CCU), agreeing they understood and agreed to be bound by the arrangements outlined by the Census Act 1920. All of these measures proved effective and will be carried forward to 2011.

6.3 Census field staff worked from one of 2 census field offices. The field offices were used by field managers to conduct operations such as recruitment interviews, field staff training, management workflow operations and for a very short time only, as a central collection point for completed boxed census questionnaires in their area. Prior to use, each field office underwent a security risk assessment to ensure appropriate physical security measures such as alarms, CCTV cameras, electronic or coded entry systems etc. were implemented.

6.4 Appropriate access controls for authorised staff were implemented in both field offices. A full closedown and decommissioning procedure was implemented for both field offices at the end of the rehearsal operation to ensure the complete removal of all materials, IT equipment etc. A similar approach is proposed for the 2011 Census. All IT equipment used by field staff, such as laptops and field PC's were tested prior to release to ensure the most secure build was established according to government security guidelines. Once returned, this equipment was sanitised to ensure recovery of any information was not possible. For 2011, a similar strategy will be adopted.

7. Print

7.1 The print process does not involve any access to confidential census information. It does however allow access to personalised information that is considered secure.

7.2 All contractors working as part of the census print operation completed pre-employment screening checks in line with the Baseline Personnel Security Standard (BPSS) and signed the CCU.

7.3 The IT systems holding personal information (such as barcode and internet access code database) were security tested and access controls implemented to ensure no unauthorised access was possible.

7.4 A secure disposal strategy for blank census questionnaire spoils was not required as all print spoils were used for testing in other areas e.g. scanner testing. For 2011 a disposal strategy for spoils is still being considered.

8. Internet Services

8.1 During the rehearsal, all contractors working on the internet services completed pre-employment screening checks in line with the BPSS and signed the CCU.

8.2 The internet services system was secured using a defence in depth approach (layers of security measures).The secure online connection between the public and the system was delivered via a trusted encryption process (secure socket layer - SSL).

8.3 Security testing, such as application and penetration testing (tests to try to hack into the system to compromise or access data), were carried out to ensure the most appropriate and robust security controls were implemented. GROS staff authorised system access to the databases (for essential system maintenance) via a strict access control policy.

8.4 In addition GROS staff were responsible for ensuring that data was securely transferred between the internet hosting site and the data processing site.

8.5 The rehearsal decommissioning strategy to re-use the existing kit within the present infrastructure was followed through successfully. This meant full secure sanitisation was not required for the rehearsal, but will be for 2011.

9. Transportation of census questionnaires (Logistics)

9.1 Blank and completed census questionnaires were transported in various ways throughout the rehearsal operation. Blank pre-addressed questionnaires (to be delivered to householders via post-out) were securely transported to the postal service provider. Both blank pre-addressed and unaddressed (replacement) questionnaires (for hand delivery to householders) were securely transported to census field staff by the logistics service provider. Completed census questionnaires were transported to the census processing warehouse in double-manned, hard-sided vehicles.

9.2 All completed census questionnaire transfers were done using dedicated logistics service provider vehicles and staff. The logistics service provider’s barcode scanning system was used to track all boxes of rehearsal questionnaires from receipt to delivery. These processes were reviewed and assured by the GROS Security Team. Due to the success of the operation, a similar approach will be used for 2011.

10. Paper Data Capture

10.1 All staff working in the PDC site underwent pre-employment screening checks in line with the BPSS and signed the CCU.

10.2 Prior to any work beginning at the site, a comprehensive security risk assessment was completed to ensure appropriate physical and procedural security measures such as alarms, CCTV cameras, electronic or coded entry systems, etc. were implemented. Robust access controls were implemented to control access into the site. In addition, access controls were implemented to ensure secure handling of the census questionnaires and to control access to the IT systems used to hold the census information.

10.3 The system used to store the scanned images at the site is a stand alone application with no external links to or from the outside world. All USB ports and other external ports to the system were disabled. Furthermore, all of the systems within the site accessing the census information underwent security testing (i.e. application and penetration testing) to provide additional assurance.

10.4 A questionnaire tracking system is used to track the whereabouts of the questionnaire throughout the scanning and data capture process. Access controls were implemented to ensure access to questionnaires was controlled, monitored and reviewed.

10.5 All data transfers from the site were authorised and conducted by established GROS staff.

10.6 The decommissioning process will include all census information in it’s varying formats. A similar approach is proposed for the 2011 Census.

10.7 GROS staff were always onsite during the warehousing and data processing to oversee the operation and in 2011 will fully manage and control the servers where the full dataset resides.

11. GROS Services

11.1 GROS in-house services during rehearsal included:

- central management of the field operations;
- central management of contracted out service provision;
- census helpline;
- conducting statistical analysis and disclosure controls on the census data;
- securely storing and controlling access to rehearsal census information; and
- IT systems for future statistical analysis work.

11.2 GROS insist that pre-screening employment checks must be completed for all staff and contractors prior to access to census information. Furthermore, an ongoing security awareness program has been established for all GROS staff to ensure they are familiar with the government data handling requirements required for census data. A security incident reporting framework is in place organisation wide to help identify and counteract any possible security vulnerabilities or incidents. Stringent access controls are applied to any area or system where census or protectively marked data is stored. Asset and configuration management and access to IT equipment and systems is strictly controlled. The network storing census information has been government assured to store information up to a restricted level. All IT maintenance contracts ensure that equipment holding census data cannot be taken off-site, but must be repaired on-site or where repair cannot be made, then the equipment remains within the care of GROS for secure disposal.

12. The Way Ahead

12.1 For 2011, we have commissioned an independent review of all systems and services for both those systems developed in-house and also for those out-sourced on behalf of GROS. Furthermore, a UK-wide independent census security review team has been established to provide additional assurance to the public of the security arrangements in place across the three census taking organisations (GROS, Office for National Statistics (ONS), Northern Ireland Statistical Research Agency (NISRA)). This review is being led by John Dowdall, the former Northern Ireland Comptroller and Auditor General.

12.2 Confidentiality is the cornerstone of the census. Census respondents need to feel assured that the personal information being collected (which they have a legal obligation to provide) will be properly protected. GROS is committed to protect, and be seen to protect, confidential personal census information throughout the lifetime of 2011 Census Programme and beyond.