2011 Census Security: Final Report to the Census Offices

Prepared by: John Dowdall, Harvey Mattinson, Peter Fagan
Last Amended: 10/06/2012
Document Status: Issue
Version: v1.0

Contents

Covering Letter

TO THE NATIONAL STATISTICIAN FOR ENGLAND AND WALES, AND THE REGISTRARS GENERAL FOR SCOTLAND AND NORTHERN IRELAND

Dear National Statistician and Registrars General,

We are pleased to present to you the final report of the Independent Review Team on 2011 Census Security.

You jointly commissioned our review in 2010 to consider the adequacy of the information assurance arrangements for the UK Censuses. The review team have substantial experience of public sector audit and information assurance. We are completely independent and our reports are public documents.

For more than two years we have had the opportunity to examine the Census arrangements as they have been planned and implemented in each part of the UK, and to scrutinise the arrangements to protect the information provided by the public. The cooperation of your Offices has, of course, been essential for our work. We have had complete access to everyone in your organisations and contractors whom we thought it necessary to meet. We have also had access to census sites and to all documentation we requested, including risk registers, audits and test results. Throughout the review, the openness of your staff and their evident commitment to ensuring the security of the censuses, has reflected the highest professional standards.

In our previous report (February 2011), we had reviewed the arrangements prior to the census date and were able to assure the public that information would be held in secure environments and that it would be handled in line with best practice and government standards. In concluding this final review of the implementation process, we are pleased to confirm that this has been the case. We were impressed that the Information Assurance operations undertaken by each Office were matched to their particular business needs. We remain satisfied, therefore, that the public can be assured that the information they have provided has been well protected. Moreover, our report points up that, in many respects, the 2011 Census can serve as an exemplar in public sector IA Management.

John Dowdall
Harvey Mattinson
Peter Fagan

May 2012

Executive Summary

This is a report to the Census Offices in England and Wales, Scotland and Northern Ireland, presenting the findings of a retrospective review of the protection applied to personal information gathered as part of the 2011 Censuses across the three organisations.

In opening, the review team wish to make the point that in submitting the Censuses to independent review, all three Census Offices have demonstrated an impressive commitment to 'transparent and accountable government'. Throughout the review period, the review team were provided with access to all relevant aspects of Census planning, preparation and execution. All key Census team members, subcontractors and stakeholders have given their time to support this work. In the experience of the review team, this is an unprecedented approach, reflecting the importance attached to Information Assurance (IA) at very senior levels within all three organisations, and the recognition that public confidence was essential for the success of the project.

In the first report from their work, the Independent Information Assurance Review (IIAR) team noted that the business environment differed for each Census Office, and hence the business processes adopted by each were necessarily different. It was also recognised that, if the IA measures taken by each were to be effective, then they should match the business processes of the organisation.

The IIAR team noted in their first report that each Census Office had indeed taken an approach to IA which matched the objectives, environment and constraints relevant to the organisation. The retrospective review presented in this second report has shown that in each case, the approach to IA has been structured to achieve cost-effectiveness, that it has been proportionate, and that it has allowed each organisation to further develop and extend its approach to IA. Perhaps most importantly for Government as a whole, in each case the lessons learned have been taken from the 2011 Census activities and applied across a wider field. It is true to say that in each case, the IA activities undertaken as part of the 2011 Census operations have acted as an exemplar, and have set a standard both within and beyond their immediate areas of business.

Overall, as a result of our review, we are very satisfied that the IA operations undertaken by each Office were matched to their business objectives and business environment, and that as a result, the personal census data gathered and handled by each was subject not only to an adequate degree of protection, but also to a degree of protection which was appropriate to individual circumstances. It is clear to the review team that the tightly focused work undertaken by each organisation has had benefits not only across the three Census Offices, but also across Government, and that the benefits will be felt for some time to come.

In retrospect, this has probably been the most rigorous census in terms of IA ever conducted in the UK. The fact that there have been no significant security incidents in the course of the project to date is not simply a matter of good luck. It is a reflection of sound IA planning which has been well implemented in the form of an effective through-life approach. We remain satisfied, therefore, that the public can be assured that the information they have provided has been well

protected and sound plans are in place to ensure that this will continue to be the case.

1. Setting the Scene

1.1. Background to the Review

The UK Censuses constitute one of the most important data collection exercises undertaken by the UK Governments. Much depends on the accuracy and completeness of the information gathered, which is used to underpin a great deal of planning and decision making in both the public and private sectors.

Public confidence that personal census information will be securely handled is a vital ingredient for success. Within the UK, census activities are undertaken by three organisations: a census for England and Wales, conducted by the Office for National Statistics (ONS); a census for Northern Ireland carried out by the Northern Ireland Statistics and Research Agency (NISRA); and a census for Scotland, carried out by the National Records of Scotland (NRS)[1]. All three Census Offices have given firm undertakings that this data will be used solely for statistical purposes, and that it will be treated in strict confidence.

Previous work[2] undertaken by the Independent Information Assurance Review (IIAR) team examined the extent to which those undertakings were being met, based on evidence available up to mid-December 2010, some three months before the Census date.

The report from that work was published in February 2011, and concluded that from the outset, ensuring the protection of the personal information provided by the public had been a core objective in the planning for the 2011 Censuses. The team were very satisfied that all three Census Offices were managing Information Assurance pragmatically, appropriately and cost-effectively. The review team were therefore confident of the ability of each Census Office to deliver their IA objectives and stated that the public could be assured that the information they were to provide to the 2011 Censuses would be well protected.

The purpose of this report, which covers the period from the initial report to the first public release of Census data is to build upon those findings, and to examine the through-life evidence relating to:

- Operations undertaken immediately prior to the Census;
- The Census activities themselves;
- The secure decommissioning and archival activities which will mark the closedown of the data gathering process.

[1] Prior to a merger with the National Archives of Scotland on 1st April 2011, this responsibility lay with the General Register Office for Scotland, GROS.

[2] http://www.parliament.uk/deposits/depositedpapers/2011/DEP2011-0257.pdf

1.2. The Review Team

The review team were chosen to provide the necessary balance of audit, security and management skills. The team was made up of:

- John Dowdall. Mr Dowdall has recently retired as Comptroller and Auditor General for Northern Ireland, responsible for independent audit of the devolved functions in Northern Ireland. He has been closely involved with the management of public expenditure and economic issues throughout his career. He was Head of the Northern Ireland Audit Office from 1994 to 2009. During this period he worked closely with the Public Accounts Committee at Westminster and, after devolution, with the Northern Ireland Assembly. He is an Honorary Member of the Chartered Institute of Public Finance Accountants and, since 2002, Visiting Professor in the School of Accounting of the University of Ulster. He was awarded a CB in 2003.

- Harvey Mattinson. Mr Mattinson spent 5 years as Head of Infosec Consultants at GCHQ before being seconded to the Cabinet Office as Deputy Director of the Central Sponsor of Information Assurance, responsible for security policy and standards, and inaugural head of the profession of accreditation. Prior to his retirement, Mr Mattinson established a number of key integrative groups in IA, including GIPSI and CIPCOG, he introduced the Claims Tested (CCTM) Scheme and he was responsible for the pan-Government accreditation of many large scale networks and services including the Government Secure Intranet, the Government Gateway, and Airwave. Mr Mattinson is a Chartered Engineer, Chartered Mathematician and Chartered IT Professional, a Fellow of the Institute of Mathematics and its Applications, and a Fellow of the BCS and Associate of the IISP. He is also an external examiner for the Government certification with the IISP, and lectures in all aspects of IA at the National School of Government.

- Peter Fagan. Mr Fagan has extensive experience in Government security, having been a founder member of the CLAS Scheme. His experience includes a number of years as the Government Gateway security manager, an extended period as lead assessor for the GovConnect programme reviewing Local Authority applications to join GCSx, and he was selected twice for the assessment of security aspects of bids for the National Lottery franchise. Mr Fagan was a key figure in the establishment of the TIGER Scheme. He has contributed to UK e-Government standards and was awarded an SC Europe prize in 2007. He has two first degrees and an MBA from Warwick Business School.

1.3. Scope of the Review

1.3.1. Introduction

The review looked into the Information Assurance (IA) activities of all three Census Offices, critically assessing the degree to which IA was being managed.

1.3.2. Areas Reviewed in this Stage

The following areas were addressed by the review team in drawing up this report:

- Accreditation prior to live operation
- Accreditation maintenance
- Security management during operations
- Information Assurance risk management
- Accreditation post-Spring 2011
- Secure decommissioning
- Secure archival

In the general case, each area was reviewed by means of interviews with key personnel within all three Census Offices, through a review of sample documentation, through interviews with personnel from key commercial partners across all three Census Offices, and via site visits to major processing centres.

Detailed descriptions are provided at Annex A.

1.3.3. Areas Out of Scope

The work was not intended to act as a 'double accreditation', nor to review the decisions of the Accreditors. It was however, intended in part to confirm for the Census Offices, that the accreditation process had been robust in each case, and that due care and diligence had been exercised in both the preparation and conduct of the accreditation exercise.

Specifically in relation to decommissioning, the IIAR team were not seeking to witness the decommissioning process itself, but rather to ensure that appropriate measures and policies had been set in place, and that there was evidence available to show that the processes were being followed, and the standards applied.

2. Findings: ONS

2.1. Business Environment

The business factor dominating the approach to IA for the ONS Census security staff was, in the opinion of the review team, the risk of a security incident reducing the effectiveness of Census operations, certainly in the run-up to the Census itself. The conduct of a Census in England and Wales reflects a significant investment, and the reliability of the data gathered is of course crucial to gaining the expected benefit. Public confidence in the secure handling of data by Government has declined in recent years, consequently any significant security issue relating to the Census would inevitably have led to public concern. A reduced response rate could have significantly undermined the cost-effectiveness of the operation, with a secondary adverse effect on the reputation of Government as a whole.

This issue affects all three Census offices. However, ONS are perhaps perceived in the national media as the face of the Census, and therefore they are in the 'firing line' should there be any perceived or actual weaknesses in the protection of Census data. This places great emphasis on the degree of assurance required in the measures and processes underpinning IA. The challenge for the ONS Census security team was to ensure that the largest single component of the 2011 Census was not disrupted by an either unnoticed, or unmanaged risk.

2.2. Key Conclusions

In the opinion of the IIAR team, the security team have risen fully to the challenge placed before them.

It appeared to the review team that the organisation had decided, at the very outset, that openness and the use of independent scrutiny would be crucial in achieving the necessary level of confidence. Acting on behalf of their consortium partners Lockheed Martin UK (LMUK), Logica were therefore commissioned to conduct extensive ISO 27001-based site audits throughout the period of preparation for the 2011 Census, and to make their reports available to ONS. At the specific request of ONS, the Centre for the Protection of National Infrastructure (CPNI) visited and reported upon security at the main data processing site. Sopra Group plc were commissioned to conduct an audit of the operational effectiveness of working practices on the 2011 Census. The ONS Census security team also conducted their own site visits. This openness clearly led to a number of benefits, but for the IIAR team it was a key indicator of the level of management commitment to establishing standards of IA which would be robust under scrutiny.

In the earlier phases of the review, the IIAR team noted that the planning and preparation for incorporating IA within ONS Census operations had consistently demonstrated a level of care which reflected both the importance of the information, and the professionalism of the individuals involved. On the basis of

the evidence made available to the IIAR team, there is no doubt that the same degree of care can be seen in the IA aspects examined in this stage.

Throughout, risks had been tracked, and a summary risk register had been maintained in order to inform executive level stakeholders; accreditation meetings had been held against an agreed agenda including a formal presentation of evidence together with a clear statement of residual risks and issues. It was clear to the IIAR team that extensive effort had been expended in order to expose and manage all relevant risks, and that approval decisions had been based on an incremental development of confidence throughout the preceding months. This reflected the sound preparation carried out by both LMUK and the ONS team, supported by a clear and well-managed through-life approach.

In cooperation with ONS Census security, on the few occasions when security briefing guidelines had been defaulted upon at the main site, decisive action had been taken. The IIAR team were impressed with the efforts of all parties not only to instil a security culture, but also to ensure that each individual felt responsible for their part of the Census. The very clear impression gained by the IIAR team was that the management of the site was very tight, and that it was based on sound experience of the effective management of risk in day to day operations.

The IIAR team note that the approach to IA demonstrated for the Census is now being incorporated into the wider ONS approach, and is providing benefits beyond the immediate business objectives of the Census itself.

2.3. Specific Detail

Purpose

The team feel that the specific points below will serve to illustrate the key conclusions of the review of ONS activities: the treatment of risk management as a business issue; and the use of a considered through-life approach.

Programme Management

The IIAR team note that ONS conducted an in-house review of their operations against the IA Maturity Model (IAMM), some eighteen months in advance of the date by which Downstream Processing (DSP) systems would need to accept live data from the 2011 Census. One of the conclusions from the review was that further work would be needed if the DSP systems were to provide a level of protection at least equal to that provided by the Census systems. Consequently, a plan to address the key points had been set in place for the DSP systems.

Discussions with the IIAR team indicated that progress against the plan was then slowed by a number of factors, some outside the control of ONS, and that as a result, it had been necessary to accept, for a short time, more risk than had been deemed desirable at the outset of the project (the review team note that the delay had been occasioned primarily by delays in the production of supporting documentation). As a consequence, for a period of approximately four weeks, the DSP systems had held a subset of Census data, prior to the award of interim accreditation.

The IIAR team were presented with evidence showing that during this period, operation of the system had been constrained to involve the minimum necessary functionality, and that it had been subject to restrictions applied in accordance with an appropriate risk management approach. The ONS SIRO had been fully involved in all aspects of the management and tracking of actions. Regular risk review meetings had been held, and considerable resources had been assigned in order to bring the systems to a point where interim accreditation could be granted, in May 2011. The IIAR team are confident that the organisation acted to manage their risks in line with best practice during this period, and note that the DSP and Census Ad-Hoc (CAH) systems have now been fully accredited for live operation.

Incident Management

The 2011 Census operations were the subject of a well-publicised, alleged breach, claimed to have taken place after Census Day, but prior to the Census Offices having completed the full paper processing stage. A claim was made on behalf of the loose collective known as LulzSec, stating that the group had gained access to entire UK census database. This turned out to have been a less than elaborate hoax, nevertheless it had the potential to severely affect the operations of all three Census Offices, and the effectiveness with which the Offices handled the incident could rightly be seen as a matter of public interest.

The IIAR team were provided with evidence regarding the management of the incident, and the decisions that were taken, comprising both retrospective and contemporary records. The evidence indicates that the incident was well managed, and that within the realities of the situation, the right people were involved at the right time, and that the defined processes were followed. In the opinion of the review team, the actions taken by ONS and their partner offices demonstrated a controlled and proportionate response, underpinned by professionalism and by very effective communications.

Secure Archiving

The archiving process for 2011 Census information begins with the production of digital records (hard disks), and microfilm images of Census returns, and concludes with their acceptance into the ONS records management system. The production of microfilm is a complex and therefore risk-prone process, involving the production of microfilm cassettes at the main data processing site, transfer to a Capita TDS site for development, and transfer of both developed microfilm and encrypted disks containing images, to the main ONS site.

The information security aspects of the planning for secure archival of ONS Census data were found by the team to be exemplary.

The review team were provided with comprehensive documentation relating to security in the archive delivery process. All deliverables from the prime contractor to ONS are listed in the documentation. Comprehensive security procedures were available, having been defined in advance of the archiving process, encompassing all delivery formats, setting out exception handling routines, and defining acceptance standards in terms of integrity and accuracy. The team were also provided with detailed procedures for microfilm production.

A status review based on the requirements of ISO 27001, relating to the procedures at the Capita TDS microfilm development site was provided, showing the implementation of an appropriate degree of security. The review team were also provided with evidence that the security implications of each option for archive production and delivery had been considered, and that residual risks had been identified and assessed prior to the adoption of a preferred way ahead.

A microfilm processing plan, produced and maintained by LMUK was also provided. The plan showed that production rates and targets were being monitored closely and on a regular basis.

3. Findings: NRS

3.1. Business Environment

The main business objectives for IA within the Census operations for NRS, in the opinion of the review team, were: to implement an appropriate level of IA in time for the Census; to carry away an increased capability for IA and for accreditation in particular, post-Census; and to achieve this within budgetary constraints. In any area of systems management this would be difficult, but in a specialised area such as IA, the problem becomes very complex.

The challenge was perhaps made more difficult by the fact that there is (and was) no formal requirement for accreditation of Scottish Government systems. Nonetheless NRS chose to pursue the accreditation route, in order to provide a consistent approach across all UK Census activities, but perhaps more importantly to ensure that Census systems in Scotland were not only secure, but were seen to be secure. That decision meant that NRS had a very steep hill to climb, not only in terms of building in the necessary business processes, but also in terms of building them into a schedule with an extremely hard end date, while still making them effective.

3.2. Key Conclusions

It was noted in the first report that NRS had adopted a business model different to that for NISRA, and different also that for ONS, choosing to maintain a more locally directed approach to IA.

This retrospective review has confirmed the benefits of the NRS approach, in that the experience gained within the NRS team is now being applied to the wider Scottish Government. As a consequence the NRS approach is being seen and adopted as an example of not only best practice for IA within that arena, but also best practice within the region on information management. The use of a more locally managed system meant that the experience became more local also; NRS, as has been noted elsewhere, drove a very cost-effective model of Census operations, and also achieved the concentration of experience into members of a team who even now are taking those skills into other areas. In the opinion of the IIAR team, that process can only increase the value of the investment in IA for the Census in Scotland.

3.3. Specific Detail

Purpose

The team feel that the specific points below will serve to illustrate the key conclusions of the review of NRS activities. The team found in particular that the effective exploitation of IA experience gained during the Census, and the adoption of a pragmatic approach to achieve a cost-effective result, were key themes.

Risk Management

The evidence presented to the review team showed that accreditation of the key NRS and CACI UK Ltd systems used for Census data gathering and processing, including systems for online entry, paper scanning and data processing, had been granted in each case, and that it had been granted prior to live data being loaded onto the system. Interim approval to operate in order to conduct limited testing had also been granted where appropriate, subject to Accreditor approval, indicating a risk managed approach to IA. The underpinning risk analyses, the IIAR team note, were based on direct experience gathered during Census rehearsals, and had in each case been updated and subsequently reviewed by the Accreditor prior to the accreditation decision. Technical vulnerability testing had been conducted on all key systems. The team also note that a number of physical site audits had been conducted by Dell SecureWorks, in addition to the security audits conducted by Logica on behalf of NRS, and the results had in each case been presented to the NRS Accreditor as further evidence of suitability for live operation.

The review team note that the formal documentation supporting the accreditation decision had been produced in parallel with other accreditation activities, when ideally it should have been produced sequentially, but note also that additional resources had been made available in order to ensure that the documentation could be provided to the Accreditor on time and against an agreed quality standard, without compromising other areas of IA. Against a background of resource constraints, the IIAR team are confident that IA aspects of the Census in Scotland were given due priority by the programme, and that a pragmatic, managed approach had been taken, which was both cost-effective and justified.

The IIAR team were provided with evidence of a comprehensive and well-maintained risk register for Census operations, which was subject to regular, scheduled reviews.

Centre of Excellence

The audit trail of accreditation activities for NRS relies principally upon the minutes of the Census Security Assurance Group (CSAG) meetings. Two streams of CSAG meetings were used: internal meetings were used as a forum for NRS decision making, whereas the external stream acted as a liaison point between NRS, their main contractor for the Census in Scotland (CACI UK ltd) and CACI's security advisors, Dell SecureWorks. Both streams of meetings were chaired by the NRS SIRO, and both the internal and external meetings were attended by the NRS Accreditor, and where appropriate, also by Logica, acting as the security advisors to NRS.

The minutes of the CSAG meetings provide the backbone of evidence regarding decision making and risk management for the NRS IA activities. However, particularly for the Census in Scotland, resources were at a premium, and the business of conducting the Census quite rightly took priority over the documentation of a formal audit trail. However, the CSAG minutes, which formed a critical part of the evidence presented to the team, had been used as an operational tool rather than an evidential record. The IIAR team therefore found it useful to adopt a 'storyboard' approach in order to work with NRS to flesh out

those notes into a fully detailed understanding of circumstances and events. The NRS team not only offered their time to follow through the storyboard approach, during an especially busy period of preparation for Census data processing, but also developed a specifically formulated response and supporting evidence. The flexibility and commitment demonstrated in this area were, the team felt, fully representative of the overall approach to IA within NRS. The key conclusions from the storyboard experience were taken on board by the Census team, they were seen to be followed through, and so the IIAR team understand, will also be adopted elsewhere in NRS and in the wider SG arena.

At the time of writing, NRS have commenced a programme of reviews on their Census activities; the IIAR team were provided with the report on the print function as an example. The report was found to be objective, and included an assessment of areas in which lessons could be learned in the wider sphere of IA, i.e. in areas outside Census operations, even though (as the review team noted), there was no security breach or incident. The team felt that this constituted evidence of a continuous improvement process, a key part of effective management of IA.

The NRS contract with CACI UK Ltd, as the prime contractor for the Census operations, was outputs-based; while this provided a degree of flexibility for both parties, it did mean that NRS were obliged to negotiate detailed requirements as the programme unfolded, including in the area of information security. This was achieved through an Integrated Project Team (IPT) dealing with security and programme risk. The more usual approach would have been to identify successful accreditation as a contractual requirement, and to monitor progress against that goal. This has been recorded by NRS as a recommendation arising from the Census operations, and will be taken forward into wider Scottish Government activities, so providing further overall benefit.

4. Findings: NISRA

4.1. Business Environment

NISRA faced some of the challenges which were faced by ONS, and also some of those which were faced by NRS, in terms of budget constraints and in terms of the application of current IA practices to a project with a ten-year cycle.

As with NRS, the main business objectives for IA within NISRA's Census operations, in the opinion of the review team, were: to implement an appropriate level of IA in time for the Census; to carry away an increased capability for IA and for accreditation in particular, post-Census; and to achieve this within the available budget. As was noted with NRS, in any area of systems management this would be difficult, but in a specialised area such as IA, the problem becomes very complex, and requires a capable management approach combined with effective utilisation of available resources.

4.2. Key Conclusions

At the outset of the Census planning stage, NISRA made a strategic decision to work with ONS on many aspects of Census operations. In the course of this review, the IIAR team have become increasingly sure that the approach taken by NISRA was the correct one to take under the prevailing business circumstances.

The IIAR team have been particularly impressed with the ability of NISRA to adapt to changing circumstances in IA, an ability which came about as a result of an approach which allowed NISRA to concentrate their resources onto areas which were specific to their business, whilst at the same time gaining the benefit of their close collaboration with ONS and their joint delivery partners.

The IIAR team note that as with NRS, the NISRA approach to IA is now being considered on a wider scale, by DFP and elsewhere, as an exemplar of best practice in the management of project-based Information Assurance. At the core of that approach is the view that IA risk and business risk need to be handled as two facets of a common issue; this is a key message underpinning effective IA, and the IIAR team were very pleased to note that it was a fundamental aspect of the successful outcome achieved by NISRA.

4.3. Specific Detail

Purpose

The team feel that the specific points below will serve to illustrate the key conclusions of the review of NISRA activities, and in particular the very sound approach to managing IA as an integrated component of programme management.

Programme Management

As part of the agreement between ONS and NISRA, it was intended that the ONS Downstream Processing (DSP) systems would be used to process both sets of

data, with a secure link provided from the ONS systems to the NISRA Census offices.

In this situation, the legal obligations on ONS to maintain control over Census data translated into a requirement for separation between data relating to the Census in England and Wales, and NISRA users granted access to the systems in order to process their own data relating to citizens residing in Northern Ireland.

Technical controls, such as those used to separate user groups on computer systems, provide functionality based on an underlying security requirement. However, IA requires that the functionality should not be taken as a 'given', i.e. it should not be assumed that the security functionality is working correctly, nor that it is appropriate. Independent testing and assessment is usually required to demonstrate both suitability and correct operation. The IIAR team understand that while it had always been the intention for ONS to provide assurance in the mechanism of separation, the delayed timescales for DSP also delayed the production of the necessary evidence.

Rather than introduce a further element of risk to the programme, ONS and NISRA jointly decided to allow downstream processing of NI Census data to be carried out solely by ONS[3], and to have the processed data transferred to a new and dedicated system sited at NISRA (the Census QA and Outputs system), for acceptance.

The decision was taken in good time to allow the implementation of the necessary additional NISRA infrastructure, together with the drafting of security documentation to act as the basis for Accreditor approval. The new NISRA system was built as a 'clone' of an existing, accredited system in order to reduce both IA and programme risk. Approval to operate was granted by the DFP Accreditor prior to live data being loaded onto the system. The evidence presented also sets out the operational constraints that were applied to the system. These include a statement that no data was to be transferred via the secure link until agreed security protocols had been put in place and tested. The team had the opportunity to examine the security procedures for data transfer, and were reassured to see that detailed project-specific documentation had been drawn up by ONS, covering the transport of encrypted disks, and the setup and management of the encrypted link.

The IIAR team felt that the risks arising from the DSP delays were well managed. The process clearly demonstrated that IA risk, programme risk and commercial risk were all managed by NISRA as different facets of the same issue. That point alone marks out the NISRA approach as an exemplar, not only in its field, but also generally.

Risk Management

The accreditation plan for NISRA, originally provided to the IIAR team for review in an earlier phase of the work, was provided again; it was clear that the plan had been maintained and updated, and the team therefore conclude that it had

[3] The review team were presented with evidence to show that the Memorandum of Understanding (MoU) between the two organisations allowed for ONS access to NI Census data, providing that there was demonstrable adherence to both best practice in IA, and to all applicable HMG IA standards.

been used to manage the accreditation and general IA processes, showing evidence of governance.

NISRA have stated to the IIAR team that they (NISRA) have been very much involved in the joint approach with ONS, and that they remained involved in the management of IA. The IIAR team were provided with evidence of regular liaison between ONS and NISRA.

The risk register for NISRA activities on the Census was also supplied for review, and showed that NISRA had adopted a joint approach on risk management, with not only their own risks identified and managed, but also any ONS risks that were relevant to NISRA operations. There was evidence that the risks were being managed, and that a 'watch list' of issues had been created and that it was being maintained.

The IIAR team note that NISRA had adopted the National School of Government (NSG) e-learning package for basic IA awareness, with two mandatory sessions held to include all Census staff. Security operating procedures were provided for review, covering the Census QA and Outputs system (the dedicated repository for NI Census data).

Evidence of security in operations was supplied in the form of a number of incident reports and associated email trails, showing a reporting line and formal resolution (a summary form having been provided in each case). The IIAR team note that the extent of the collaboration between NISRA and ONS meant that in fact, very few incidents were specific to NISRA, and the evidence provided therefore relates primarily to operational issues. NISRA have pointed out to the IIAR team that a joint incident management process existed throughout the Census operations, and it was clear from the IIAR team's review of the ONS incident management records that NISRA had been involved and active.

As a result of the joint approach taken by NISRA and ONS, the scope of any decommissioning activities specific to NISRA was much reduced, to the extent that until one of the in-house systems is retired, no major decommissioning activities will be required, at least in relation to the 2011 Census. The IIAR team note however, that the main building used to house completed returns has now been decommissioned, and that a completion audit has been conducted.

Annex A: Areas Addressed in this Report

Accreditation Prior to Live Operation

It is a requirement for Government systems that they should be accredited (i.e. approved for operation against an agreed security target), prior to live data being loaded onto them[4]. In relation to the systems used to support paper-based and online Census activities, the team sought to verify that:

- All systems holding personal census data had been accredited prior to any live data being loaded;
- All related risk acceptance decisions made by the Census Offices had been made on an informed basis;
- The accreditation decisions had been based on a sound risk assessment and review process.

Accreditation Maintenance

Accreditation is not an event, but rather an ongoing activity to ensure that the overall level of risk remains within the risk appetite of the organisation; consequently a well-managed approach to IA will include ongoing reviews and assessments. A well-managed approach will ensure that changes are made on a controlled basis, that the security impacts of changes are considered prior to implementation, and that where necessary, testing is carried out in order to confirm an acceptable level of risk.

In this respect the review team sought to verify that:

- Accreditation had been managed as an ongoing process, in line with applicable HMG standards and best practice;
- Changes to the risk profiles of systems holding personal census data had been monitored and reviewed for acceptability;
- Changes to risk profiles had been subject to formal acceptance prior to implementation;
- Where necessary, system vulnerability assessments had been carried out as part of the implementation of changes, and that the process had encompassed a review of accreditation status, levels of outstanding risk, and overall acceptability.

The review team also sought to confirm that these processes formed a component of overall Census operations and could be relied upon to be effective in ongoing Census activities.

[4] Exceptionally, a system may be approved to run without full accreditation, where the risk is deemed to be known and acceptable, and where actions are known to have been initiated that will reduce the risk to within the stated levels, within an agreed timeframe.

Security Management During Operations

The IIAR team examined the effectiveness of ongoing security management during operations, specifically incident management, seeking to verify that:

- An appropriate level of security management had been included within 2011 Census operations;
- An effective incident handling process had been a part of the 2011 Census operations;
- Any incidents affecting personal Census data had been dealt with in an effective manner;
- A 'lessons learned' process had been a part of the 2011 Census operations;
- Census operations had included a process to identify and implement any steps needed to reduce the likelihood of re-occurrence of an incident.

The review team also sought to confirm that these processes formed a component of overall Census operations and could be relied upon to be effective in ongoing Census activities.

Information Assurance Risk Management

Although it is important to be able to learn lessons from actual and suspected incidents, prevention is deemed to be better than cure. Therefore the IIAR team also sought to verify that:

- In addition to the processes already identified by other review activities, an additional process had been in place, assessing new and changed threats leading potentially to increased levels of risk;
- There had been in place a supporting review mechanism identifying previously unknown vulnerabilities which might also have led to increased risk;
- There had been in place a process for taking review information and using it to inform operational decisions, accreditation status decisions, and the process of overall risk management.

The review team also sought to confirm that these processes formed a component of overall Census operations and could therefore be relied upon to be effective in ongoing Census activities.

Accreditation Post-Spring 2011

Following the paper data gathering process, and the reconciliation of that information against the data gathered via the Internet, the processing of Census information includes a stage in which it is anonymised into a non-disclosive database that can then be used to carry out statistical analyses.

As part of this, the information is adjusted to ensure that no individual or small group of individuals can be identified from the Census outputs, even where there is a degree of prior knowledge; that is, steps are taken to ensure that it will not be possible to selectively refine searches in order to produce a set of results where that result can only apply to one (known) individual.

These activities form components of 'downstream processing' (DSP). All three Census Offices undertook to ensure that downstream processing systems, although they would not be needed on Census Day itself, would nonetheless be approved for operation prior to having live data loaded onto them. Just as for the systems required for Census day, the IIAR team therefore sought to ensure that:

- All relevant systems, particularly those holding personal census data, had been accredited prior to any live data being loaded;
- All related risk acceptance decisions made by the Census Offices had been made on an informed basis;
- The accreditation decisions had been based on a sound risk assessment and review process.

Secure Decommissioning

HM Government standards, and other accepted sources of best practice (such as the international standard for Information Security Management, embodied in the ISO 27000 series), stress the importance of those processes which ensure that disposal of unwanted IT equipment does not also lead to accidental disposal and therefore compromise of, the data stored on the equipment.

In relation to personal census data, the review team were therefore concerned to verify that:

- All relevant systems and system components, and all other components holding personal census data, had been appropriately cleansed and or/made inaccessible, prior to disposal and/or re-use;
- Access control had been maintained over systems and data to ensure no unauthorised access prior to confirmation of data cleansing;
- Appropriate destruction/disposal mechanisms and appropriate methods of data cleansing had been employed.
- A process had been defined for the demonstrably secure disposal of paper questionnaires.

The review team also sought to confirm that these processes formed a component of overall Census operations and could be relied upon to be effective in any relevant future processing of Census data.

This part of the review was deemed to include:

- Systems holding personal census information at processing centres and back-up sites;
- Online census data gathering systems;
- Field laptops and other systems used to support field operations;
- Systems and databases holding non-Census personal information, such as those related to recruitment, training and payroll for field staff;
- Downstream processing systems, as previously described.

Secure Archival

At the conclusion of the main data processing activities, Census data will be archived by each Census Office. Clearly, any breach affecting the archived data could have the same impact as a breach of the live systems. Therefore the review team sought to verify that:

- Arrangements for archiving the information provided for the 2011 Census included appropriate measures relating to Information Assurance;
- Those arrangements were in line with all relevant legal and regulatory requirements;
- There was a well-defined scope setting out that material which was to be archived, and that which was to be disposed of.

This examination was deemed to include:

- Microfilm images of census returns (agreed by the relevant national archive organisations as the appropriate medium for archival purposes);
- Electronic images in e.g. an Image Viewing System (IVS);
- Payroll information for census field force, with a potential requirement to keep that information for a period.

Glossary

BCS	British Computer Society
C&W	Cable and Wireless
CAB	Change Approval Board
CAH	Census Ad-Hoc (system)
CCTM	CESG Claims Tested Mark
CESG	Communications Electronic Security Group
CIPCOG	Civil Information Assurance Products and Services Co-Ordination Group
CLAS	CESG Listed Adviser Scheme
CoCo	Code of Connection
CPNI	Centre for the Protection of National Infrastructure
CSAG	Census Security Assurance Group (NRS)
CSB	Census Security Board (ONS)
DFP	Department of Finance and Personnel
DSP	Downstream Processing (system)
GCHQ	Government Communications Headquarters
GCSx	Government Connect Secure Extranet
GIPSI	General Information Assurance Products and Services Initiative
GSi	Government Secure Intranet
HMG	Her Majesty's Government
HMRC	Her Majesty's Revenue and Customs
IA	Information Assurance
IAMM	Information Assurance Maturity Model
IAO	Information Asset Owner
IIAR	Independent Information Assurance Review
IDC	Internet Data Capture
IISP	Institute of Information Security Professionals
IPT	Integrated Project Team
ISO	International Organisation for Standardisation
IT	Information Technology
IVS	Image Viewing System
LMUK	Lockheed Martin UK

LS	Longitudinal Study (system)
MBA	Master of Business Administration
MoU	Memorandum of Understanding
MSc	Master of Science
NICS	Northern Ireland Civil Service
NILS	Northern Ireland Longitudinal Study (system)
NISRA	Northern Ireland Statistics & Research Agency
NRS	National Records of Scotland
NSG	National School of Government
ONS	Office for National Statistics
PDC	Paper Data Capture
QA	Quality Assurance
RMADS	Risk Management and Accreditation Documentation Set
RPT	Recruitment, Payroll and Training
SC	Secure Computing
SIRO	Senior Information Risk Owner
SyOPs	Security Operating Procedures
TDS	Total Document Solutions (part of the Capita group)
TIGER	A not-for-profit security tester certification scheme
UK	United Kingdom