General Register Office
for
SCOTLAND
information about Scotland's people

logica
be brilliant together

SCOTTISH CENSUS
INDEPENDENT SECURITY REVIEW
REPORT

Issue **1.0** Date **24/03/2011**

Logica is a business and technology service company, employing 39,000 people. It provides business consulting, systems integration and outsourcing to clients around the world, including many of Europe's largest businesses. Logica creates value for clients by successfully integrating people, business and technology. It is committed to long term collaboration, applying insight to create innovative answers to clients' business needs.

Logica is listed on both the London Stock Exchange and Euronext (Amsterdam) (LSE: LOG; Euronext: LOG).

More information is available at www.logica.com.

CONTENTS

1 MANAGEMENT SUMMARY

1.1 Introduction

At the heart of Scotland's Census programme is the need to keep respondents' personal data secure and safe from compromise. The success of Scotland's Census relies on the public trusting the General Register Office for Scotland (GROS) to look after their data.

Good security management encompasses a broad range of areas including procedural, physical and personnel controls as well as technical measures. Only by operating a 'defence in depth' approach can an organisation ensure that they are exposed to minimal risk of a compromise.

Fundamental to security governance is the principle of risk management. Realistically, it is often impossible to eliminate all security risks within a system or process and instead, the focus has to be on reducing the risk to a level which is acceptable to the organisation.

Logica was contracted by GROS to provide an independent security review of processes in place to manage the 2011 Census and 2009 Census rehearsal.

This report is intended as a summary of our findings with respect to the security strand within the Census programme. It takes into account the programmed assessments Logica has conducted as well as anecdotal observations during the time we have been working with GROS.

1.2 Approach

For the last two years, Logica has been observing and assessing GROS activities in support of Scotland's Census.

A large part of this work has been programmed assessments. These have been targeted at specific areas of Census operations where GROS required additional assurance that good security practices were being followed and they were not exposing themselves to unacceptable risks.

These assessments were carried out during the 2009 Census Rehearsal as well as the 2011 Census and are summarised in Section 3, below.

At the time of writing, it is still intended to carry out further assessments in respect of downstream processing in due course. This report purely covers activities and notes observations up to March 2011 and the immediate lead up to Census Day.

1.3 Observations

Security has been placed at the heart of Scotland's Census 2011. It is a central strand running through all areas of the Census operation and has been considered at key points in the programme.

At the same time, GROS has introduced an Information Assurance governance regime which ensures that security practices are in line with national policy as defined by the Cabinet Office.

This approach ensures that risks are appropriately monitored, managed, escalated and addressed by appropriate staff within the Census programme.

During the two years we have worked with GROS, we have seen an increasingly mature approach to Information Assurance and in line with this, a lower threshold for the tolerance of operational risks, whether internally or in relation to services delivered by its partners.

This pragmatic and systematic approach to security has resulted in a Census programme which appears to have appropriately addressed residual security risks in relation to the handling of personal data.

The Scottish public should be confident that the processes underpinning Scotland's Census take due consideration for the protection of their information.

1.4 Acknowledgements

We would like to thank all the staff working on the Census, both within GROS and its partner organisations, who have been very open and have allowed us to observe their work, often whilst they were at critical points in the programme.

Particular thanks must go to the Census Security Team for all their assistance and co-ordination throughout this programme of work.

2 BACKGROUND

2.1 The Scottish Census 2011

Scotland's Census will take place on 27 March 2011. The Census is undertaken every 10 years to create a picture of Scotland's populace and society. It is organised by the General Register Office for Scotland (GROS).

The questions asked by the Census not only build an understanding of the characteristics of people and households, they also help in informing how public services are allocated and targeted in the years to come.

2.2 Logica

Logica is the UK leader in information security management – one of the first organisations to obtain BS7799-2 certification and has continued to be certified to ISO27001 and ISO9001.

Logica has over 400 security and business consultants in the UK certified with recognised qualifications such as CISSP, SABSA, CISM, CISA and CLAS. Globally Logica has over 1000 Security staff operating out of nine centres of excellence worldwide, offering a "Boardroom to Bytes" services that is unrivalled in any market sector.

Logica's engagement on Scotland's Census was led by Tony Kelly, one of our CLAS Consultants.

2.3 Requirements

Logica was asked by GROS to provide an 'Independent Security Review for the 2009 Census Rehearsal and the 2011 Census in Scotland'.

The main purpose has been to provide assurance to the public and Scottish Government that the exercise is being completed securely, and that GROS can be 'trusted' with the public's information.

2.4 Approach

Logica has worked with GROS in undertaking a number of targeted risk assessments during both the 2009 Census Rehearsal and 2011 Census. These have been primarily conducted in areas where the Census Security Team required additional assurance that risks were being appropriately considered.

In carrying out these assessments, we have worked with GROS staff in assessing 'in-house services' as well as partners where they have responsibility for delivery. More details on the assessments can be found in Section 3, below.

Additionally, Logica's CHECK Team has conducted programmed Penetration Testing on a number of systems supporting the Census operation. A number of other CHECK Teams have also carried out testing activities during the programme to provide a comprehensive series of tests at critical times during key system life cycles.

2.5 IRIS

In order to assess the requirement for security related procedures, processes and controls, it is necessary to assess the sensitivity of the information that is being handled and how a breach of confidentiality, integrity or availability could affect the programme.

Where appropriate, we used Logica's internally developed risk assessment tool IRIS as a basis for a number of the assessments.

IRIS allows us to assign value to the Business Processes and measure the operational impact in the event of a security incident.

2.6 ISO27000

Underpinning IRIS are the control measures within international information security standard ISO/IEC 27002:2005. Part of the ISO27000 series of security standards, ISO27002 comprises a 'Code of Practice for Information Security Management'.

Within ISO27002 is a list of controls designed to support best practice in the implementation or maintenance of an Information Security Management System (ISMS).

These controls address the risks to confidentiality, integrity and availability across all areas of security (technical, physical etc).

2.7 HMG Information Assurance Policy

GROS operates within the context of the Scottish Government's devolved administration powers and is subject to overarching Scottish Government Information Assurance requirements, particularly in respect of technical and personnel security.

The Scottish Government's approach to Information Assurance is in line with HMG IA Policy, as published by the Cabinet Office.

As such, the assessments were mindful of HMG IA Policy and where appropriate, assessments were conducted against HMG IA requirements.

2.8 Scope

This report is primarily based on findings and observations from programmed assessments carried out by Logica staff during the 2009 Census Rehearsal and 2011 Scottish Census.

It also takes into account observations and information gleaned over the last two years in working with the GROS Census Security Team and its partners.

At the time of writing, Logica have also been asked to assess downstream processing activities (data cleansing, secure sanitisation, anonymisation etc) which will be undertaken after 2011 Census data gathering activities have ceased. These areas are out of scope of this report.

3 PROGRAMMED SECURITY ASSESSMENTS

Throughout the 2009 Census Rehearsal and 2011 Scottish Census, Logica conducted a number of security assessments across key areas of the programme.

The aim was to identify any residual risks which might be considered unacceptable by GROS, specifically in areas where the Census Security Team required additional assurance.

3.1 2009 Census Rehearsal Field and Payroll Services System Risk Assessment

A key part of the 2009 Census Rehearsal programme was the Field and Payroll Services System, which underpinned the operation of field activities. This system was able to track field processes, allocate and manage tasks for Field Staff as well as record and process their expense claims.

The work was conducted between February and April 2009 using our risk assessment and compliance tool IRIS.

Results were also measured for compliance against applicable HMG Standards.

The overall findings were positive, with no High priority Recommendations made. A number of Medium and Low Recommendations were identified, which were grouped into 3 key themes:

1. Processes to be put into place to manage the remote updating of Anti Virus signature files by laptop users
2. Clarity of responsibilities and remit between the system hosts and GROS with respect to specific tasks
3. Business Continuity plans for the system hosts and GROS to be benchmarked to ensure parity and avoid gaps

It is understood these issues were resolved. Another provider will host the service for the 2011 census.

3.2 2009 Census Rehearsal Field Enumeration Risk Assessment

GROS requested that Logica conduct a security review of Field Enumeration processes for the 2009 Census Rehearsal. The assessment was conducted in March 2009, again using our IRIS risk assessment and compliance tool. Additionally, consideration was given to compliance with applicable HMG Information Assurance Policy and Standards.

A number of Medium and Low risks were identified which, once again, were grouped into key themes:

1. Secure storage of collated completed Census Questionnaires at Field Enumerators' home addresses.

2. Co-ordination of Business Continuity plans for Field operations within the overarching Census BC strategy.

3. Additional background checks on Field Staff to supplement existing vetting checks.

With respect of the first recommendation, it is understood this is a legacy process which has been used in the design of previous Scottish census taking operations. Additionally, the requirement for Enumerators to use a lockable room or container has been specified within employment contracts. The residual risk was accepted by the Census Security Assurance Group.

Processes were subsequently introduced to mitigate the risks around the last 2 points.

3.3 2009 Census Rehearsal Paper Data Capture Site Security Assessment

During the 2009 Census Rehearsal, completed questionnaires were collected, scanned and processed at a central location. The facility was provided and maintained by CACI (UK) and was intended to demonstrate the stability, reliability and integrity of processes that could then be scaled up for the 2011 Census.

A site visit and security assessment was conducted in August 2009. The site was inspected using the Cabinet Office protective security assessment matrix, in parallel with an assessment of the supporting processes.

The site and its underlying processes were found to be more than adequate and the methodical and risk-cautious approach to security was demonstrated by the fact that only one minor risk was identified in relation to emergency lighting, which was subsequently addressed.

3.4 2011 Census Internet Data Capture Site Assessment

Part of the 2011 Census programme will involve a service where the public can complete their Census Questionnaires online. To support this, an Internet Data Capture (IDC) service has been provided by Brightsolid and TNS.

As part of its security review, Logica was asked to conduct an assessment of the facility hosting the IDC service. The assessment consisted of a physical protective security inspection of the site in September 2010 and a subsequent review of Brightsolid's security policies and procedures.

A small number of observations and recommendations were made and these have been managed through the Census Security Assurance Group (CSAG) forum.

The assessment found overall a very good level of security integrated into Brightsolid's working practices. Physical security procedures at the site appeared robust and sufficient to mitigate any significant risk of attack or intrusion.

The overall findings reflect the fact that security has been considered as an integral factor in the IDC phase of the 2011 Census programme.

3.5 2011 Census Field Office Security Assessment

At the centre of the 2011 Census programme is Field Operations, the logistics surrounding the delivery and subsequent collection of Census questionnaires.

In October 2010, a site visit of a representative Field Office was undertaken.

The assessment consisted of a physical protective security inspection of the site and consideration of supporting security procedures in place for Field Operations.

A small number of observations and recommendations were made and these have been managed through the CSAG forum.

Overall, it was felt that the risks in storing a large number of bulk completed questionnaires in one location were being adequately addressed using a combination of physical, personnel and procedural security measures.

Staff at the site displayed good knowledge of security awareness and had integrated processes which provided additional assurance, mitigating the risk of compromise at the site.

Through discussions at CSAG, it is understood these processes are reflective of those in place across all Field Offices and where a specific location presents an issue, the Census Security Team are involved in discussions with Facilities Management to provide advice and assistance.

3.6 2011 Census Paper Data Capture and Coding Site Assessment

A key element of the 2011 Scottish Census programme is the accurate capture and recording of questionnaire returns from respondents.

To provide a secure means of facilitating these processes, a Paper Data Capture and Coding (PDC) Site has been created. The design and operation of the site build on the experience gained in running a similar site during the 2009 Rehearsal (see 3.3, above). However, a much larger site is being used as the operation has scaled up significantly. The specification and security features of the site have been designed by CACI (UK) in consultation with their security partners, Dell SecureWorks.

Logica conducted an assessment of the facility in November 2010, which consisted of a physical protective security inspection of the site and supporting procedures.

One minor recommendation was made which has since been resolved.

The overall findings were that both the PDC Site and supporting operations appeared to incorporate security considerations appropriate to the sensitivity of the data being processed.

Physical security procedures were seen to be robust and proportionate to the threat landscape the Census is operating within.

Similarly, supporting processes were designed with the intention of introducing and maintaining a high level of security, but still pragmatic and conducive to the primary functions to be carried

out at the site. A true 'defence in depth' approach has been designed into PDC operations which should ensure that any residual risk is minimal.

3.7 2011 Census Helpline Contact Centre Assessment

GROS has introduced a Helpline service to support members of the public who have difficulty or questions in completing their questionnaire, or who require advice on other Census matters.

In February 2011, Logica carried out an assessment of the procedural, physical, technical and personnel security measures underpinning the Helpline service.

A small number of minor observations and recommendations have been made and at the time of writing it is understood these are to be considered by CSAG.

4 SECURITY OBSERVATIONS

4.1 GROS Approach to Security

It has been apparent throughout Logica's work with GROS that security has been placed at the heart of the running of the 2011 Census.

Within the past few years, we have seen the Census Security Team becoming increasingly involved across all areas of the programme, ensuring that workstream managers are aware of their responsibilities and integrate good security practice within their areas.

A fundamental part of this has been the development of a security forum, the Census Security Assurance Group (CSAG, see below).

Additionally, in the time we have worked with GROS, we have seen information assurance practices become more closely aligned with HMG Information Assurance Policy. Now, each major information system, whether internal or externally supplied, must have a Risk Management Accreditation Document Set (RMADS) in line with the requirements of HMG Information Assurance Standard 2. In line with the Standard, residual risks are considered by the GROS Accreditor and SIRO, and managed through the CSAG Risk Register where appropriate.

All this has been undertaken by a relatively small team and it is to their credit that the Census Security Team and GROS security staff have managed to introduce a structure which ensures that security is considered in all appropriate areas of the business to the extent where it has become an integral part of Census processes.

4.2 Census Security Assurance Group

GROS has introduced two security forums dealing with internal functions and external delivery partners respectively.

Both internal and external meetings follow a similar format in having an agenda that primarily deals with the collated risk register. This ensures that risks are not missed, and where remedial action is required, this is actively tracked through successive meetings until the matter is satisfactorily resolved.

The methodical and systematic review of the risk register at every meeting is seen as best practice and ensures that risks raised across the business, or from other areas such as our programmed assessments (See Section 3, above) or the Independent Information Assurance Review (IIAR) Team (see 4.6, below) are properly monitored, managed and where applicable, resolved.

The GROS Accreditor and SIRO sit on both forums to ensure they are properly sighted of risks and are able to give informed decisions where required.

4.3 Penetration Testing

In parallel to the risk reviews and site visits Logica has undertaken, there has been an ongoing programme of Penetration Testing activity to provide technical assurance that the systems and services supporting the 2011 Census (and prior to this, the 2009 Census Rehearsal) are suitably robust and secure.

The tests have been carried out by CESG approved CHECK Penetration Test teams[1] to ensure that the work has been of a consistent nature and is informed by current HMG IA Policy. Checks have been carried out on critical systems at appropriate times, i.e. when the build is representative of the final system, but still allowing time for any remedial action as necessary.

Where issues have been raised, these have been assigned to responsible staff either internally within GROS or externally to the service provider as appropriate and once again these have been managed and monitored through CSAG.

The technical assurance provided by such activities has become increasingly important as there has been an evident move towards the use of online channels to support public response to the 2011 Census. As the programme has progressed, there has been an appreciation that a large part of the public will want to interact over the internet and as such additional assurances are required to ensure that this transaction will be just as secure as the processes in place supporting the return and coding of hard copy questionnaires.

4.4 Pragmatic Risk Management

The field of security risk management relies on making informed decisions on protective measures to mitigate risks. In some cases, the likelihood of the risk coming to pass (i.e. the vulnerability being exploited) is relatively low, but nonetheless it may be prudent to introduce the control in any event due to the impact if the exploit were to be realised.

Against a backdrop of increased financial restraints in the public sector and greater accountability for public spending, it has become more difficult to justify large spends on protective security measures, when there is a significant chance they will not ultimately be relied upon.

Therefore, a level of pragmatism and realism is required when considering security controls. Within CSAG, this practical approach is regularly demonstrated. Given the relatively short duration of most phases of the Census programme, judgements are taken on the cost benefit as well as the effectiveness of the control.

4.5 Delivery Partners

Although GROS is running a significant part of the 2011 Scottish Census using in-house resources, the success of the programme relies to a large extent on services provided by delivery partners, particularly CACI (UK) who are providing systems which underpin several of the key services, including data capture and coding.

[1] http://www.cesg.gov.uk/products_services/iacs/check/index.shtml

For the 2011 Scottish Census, CACI (UK) has partnered with Dell SecureWorks to provide security services.

From the start, the approach by CACI (UK) and Dell SecureWorks has been to meet, and often exceed, HMG IA baseline requirements in respect of security controls. Certainly, their RMADS display a minimal appetite for residual risk, with thorough and rigorous controls in place.

Physical security inspections of CACI (UK) sites in support of Scotland's Census 2011 illustrate their 'defence in depth' approach. There is a high level of assurance and a methodical approach to security management apparent in all their work, which provides additional assurance to GROS in using their services.

In their role as primary external partners on the External CSAG forum, CACI (UK) and Dell SecureWorks appear to be open in communicating issues to GROS, however minor and often present proposed solutions so the group can consider how best to resolve the matter.

4.6 Independent Information Assurance Review Team

In order to provide assurance that personal data being collected in all three Censuses (the Scottish Census, the Office for National Statistics Census for England and Wales, and the Northern Ireland Statistics and Research Agency Census for Northern Ireland), an Independent Information Assurance Review was undertaken.

This review examined all three census operations to ensure that a common baseline level of information assurance was being applied.

The report is published on the GROS website[2] and states that the Review Team had no concerns with the processes underpinning the Scottish Census 2011 and that, in their words:

"The review team are confident that the central base of accumulated skills and aggregated experience are sufficient to meet that challenge, and to provide a level of protection for personal information which will exceed expectations"

The findings of the IIAR Team tally with those of the Logica team in finding no fundamental issues or areas of concern, and in appreciating the excellent work being done within the Census operation.

[2] http://www.gro-scotland.gov.uk/files2/the-census/policy/2011-census-security-report-irt.pdf

5 SUMMARY

The view of the Logica Independent Security Review Team is that security is visibly at the core of Scotland's Census 2011 and every effort has been made within GROS and its partners to ensure that the risk of security incident has been minimised within each stage of the Census operation. This should continue up to Census Day and beyond, as ongoing audit and compliance checks will be undertaken throughout the programme.

We have had the pleasure of working alongside GROS for over two years in conducting this independent assessment. In that time, GROS' approach to Information Assurance has visibly matured, primarily due to the dedicated efforts of the Census and wider GROS Security Team. They have done so with limited resources in parallel to their primary duties of dealing with 'routine' day to day issues across the Census operation.

This approach has been broadly in line with the requirements of the HMG Information Assurance Maturity Model (IAMM)[3], which measures and monitors public bodies' progress against the Information Assurance requirements of the National IA Strategy.

The move to embed security and specifically HMG IA Standards at the heart of what GROS do has seen the implementation of a structured accreditation and risk management process. Key corporate systems supporting the Census are subject to risk assessment, the results of which are recorded in Risk Management Accreditation Document Sets (RMADS), as required by IA Standard 2. Decisions on accreditation and risk acceptance are taken by the Accreditor and SIRO, who monitor progress in regular CSAG meetings.

Security can therefore be seen to be the cornerstone of the Census programme, reflecting the importance attached to preserving the confidentiality, integrity and availability of Census data.

Given that the 2011 Census is operating against a climate of ever increasing public concern over government bodies 'holding' citizen data securely and where campaign groups are actively discouraging the completion of Census questionnaires, it is of vital importance that GROS are able to provide assurance to the public that their information will be held with due regard to security. The Census relies on the public being open and forthcoming in their responses.

The findings of this Independent Security Review are that GROS and its partners have taken all reasonable steps to preserve the security of public information entrusted to them and that the public should be assured that their data will be handled accordingly.

[3] http://www.cesg.gov.uk/products_services/iacs/iamm/index.shtml

A. Glossary

BC	Business Continuity
CESG	Communications Electronic Security Group
CHECK	CESG IT Health Check Scheme
CISA	Certified Information Systems Auditor
CISM	Certified Information Security Manager
CISSP	Certified Information Systems Security Professional
CLAS	CESG Listed Adviser Scheme
CSAG	Census Security Assurance Group
GROS	General Register Office for Scotland
HMG	Her Majesty's Government
IA	Information Assurance
IAMM	Information Assurance Maturity Model
IDC	Internet Data Capture
IEC	International Electrotechnical Commission
IIAR	Independent Information Assurance Review
IRIS	Logica Risk Analysis Tool
ISMS	Information Security Management System
ISO	International Organization for Standardization
IT	Information Technology
NISRA	Northern Ireland Statistics & Research Agency
ONS	Office for National Statistics
PDC	Paper Data Capture and Coding
RMADS	Risk Management Accreditation Document Set
SABSA	Sherwood Applied Business Security Architecture
SIRO	Senior Information Risk Owner
TNS	Team Netsol Ltd