Bridewell CONSULTING

2019 Census Rehearsal

Independent Information Assurance Review

July 2019

Background

The UK Census has taken place every ten years or thereabouts since 1801. It provides a detailed snapshot of the population that enables central and local government to develop policies, plan and run public services, and allocate funding. It also helps businesses to better understand their customers to make important commercial decisions, as well as supporting research and community groups. The UK population is approximately 67 million in 27 million households. Timely and accurate completion of the Census is required by law, with fines up to £1,000 for non-compliance.

Since the 2011 Census, the use of citizen data across the UK has expanded significantly across all sectors of life. Citizen data will be processed by electronic means to a greater extent than ever before. The proliferation of data and connectivity in that time has seen an associated growth in the occurrence and awareness of data breaches. Subsequently, the level of public reassurance required concerning the protection and handling of citizens' data remains very high.

In 2010 the Office for National Statistics (**ONS**), the Northern Ireland Statistics and Research Agency (**NISRA**), and the National Records of Scotland (**NRS**) jointly commissioned a review of the adequacy of the information assurance arrangements for the 2011 UK Censuses. The purpose was two-fold: to ensure that citizen data was appropriately protected, and to provide the public with confidence in the protection of citizen data collected during the Census.

The next Census will take place in 2021.

Independent Information Assurance Review

In 2019, with approval from the UK Census Committee, the three Census bodies undertook a commercial tender supported by the National Cyber Security Centre (**NCSC**). That tender resulted in a contract being awarded to Bridewell Consulting Limited to conduct a independent information assurance review ahead of the autumn 2019 Rehearsal.

Bridewell Consulting are certified by the NCSC to provide cyber security consultancy services including Audit and Review. Bridewell Consulting utilised an evidence based assessment approach to ascertain whether controls were designed and operating effective. The assessment itself was divided across a number of high level areas, which then split into lower level information security controls, which focused on governance, risk assessment and management, security operations and security assurance**.**

The review took place throughout April, May and June 2019. The review involved a series of interviews and system demonstrations with personnel within each Census body and their suppliers, assessment of extensive documentation, and observation of key information security controls in operation. Bridewell developed a series of interim reports, which highlighted a series of findings and remedial action, and ratification of remedial action taken in response to those interim reports.

This report represents the concluding output of the review, which is intended to provide an overview of key assessment approach and outcomes.

Executive summary

Throughout the course of this review, all three Census bodies have been open and forthcoming, which coupled with the voluntary engagement of this review demonstrates a commitment to a transparent and accountable government. All three Census bodies have demonstrated comprehension of the importance of assurance through their objectives and priorities; to protect and to be seen to protect citizens' personal data.

All stakeholders and personnel have readily given their time and have been responsive to requests for evidentiary material in support of this review. All personnel involved have been receptive to ongoing commentary, observations, and recommendations.

Many of the systems for digital data capture, transfer, storage and processing are still in early design and delivery stages. Some components of the 2021 Census environments are not intended to be operational for the 2019 Rehearsal. As such, some elements of this review assess the principles and procedures for system development, threat identification, and risk mitigation.

The primary areas of review have been the online environments for online questionnaire completion and submission, in-house environments for data hosting and processing, data transfers, system development, risk management and supplier assurance. Areas not assessed in-depth, but which should be scrutinised between 2019 Rehearsal and 2021 Census include postal questionnaire services, fieldwork services and contact centres.

While some deficiencies have been identified throughout the review, the responsiveness and ownership of remediation has been impressive to the extent the review team are satisfied that all such deficiencies have been resolved or that a viable and timely course of resolution has been established.

Office for National Statistics

NISRA
Northern Ireland Statistics and Research Agency
Gníomhaireacht Thuaisceart Éireann um Staitisticí agus Taighde

National Records of Scotland

Security governance

Effective security must be driven from the top down. It must be demonstrated and embedded through actions, decisions, and ownership at senior levels.

Senior and executive management are actively informed and involved in security matters at **ONS** and **NISRA**, with standing agenda items and attendance at oversight boards. Senior oversight at **NRS** is maturing to bring them into line with their peers.

Supplier assurance

Where activities are outsourced, an agreed baseline of security requirements and evidence of compliance with those requirements is essential to maintain overall assurance of security.

All three Census bodies demonstrated a robust set of security requirements, which were developed in accordance with industry good practice, both for the suppliers' own systems and for systems being developed by those suppliers. Due diligence checks and ongoing assurance of supplier compliance with security requirements is effective within each Census body.

ONS have dedicated resources for supplier due diligence, including on-site assessments and self-attestation of ISO27001 security requirements as a baseline.

NISRA rely on **ONS** for most key service providers; **NISRA** are intrinsically involved with **ONS** in defining supplier requirements and work closely with **ONS** for ongoing assurance.

NRS conduct due diligence against key suppliers at the point of inception and maintain regular interaction.

Roles & responsibilities

The ability to deliver key security functions effectively and consistently is dependent on adequate availability of appropriately skilled resources.

ONS demonstrate both suitable capacity and capability, with distinct dedicated roles across governance, risk management, and security operations. These were discussed at length and contrasted against industry good practice and frameworks.

NISRA demonstrate adequate resource capacity given the comparative size of the organisation, and their dependency on **ONS** for core systems. Security capability is maturing through recruitment and consolidation of security roles into a single team.

NRS demonstrate appropriate capability, and recruitment is in progress to increase resource levels to deliver adequate capacity within the Census security and assurance function.

Risk management

Complete security is not viable in any complex operation, so the objective of security is to reduce the likelihood and impact of adverse events to tolerable levels.

Risk identification, assessment, treatment, ownership, and reporting at **ONS** are well designed and operating effectively, using established industry procedures and independent expert advice.

Risk assessment, ownership and reporting at **NISRA** use a straightforward procedure that is adequate for a small organisation. Effective identification of threats and risk mitigation is maturing.

Risk identification, assessment, and treatment at **NRS** are effective. Risk ownership and reporting is maturing.

Security operations

Effective security requires controls and procedures that are well defined and that are implemented consistently and in accordance with those designs. It is of equal importance that the design adequacy and operational effectiveness can be meaningfully demonstrated to stakeholders.

ONS demonstrates strong operational capability and capacity, with distinct dedicated roles across design, support, monitoring and assurance. **NISRA** and **NRS** have engaged third parties for IT and security operational support; assurance oversight of these third parties is maturing within each Census body.

Monitoring & alerting

The ability to promptly detect and respond to malicious or suspicious activity can significantly affect the outcome or severity of an incident.

ONS demonstrate effective security monitoring capabilities for internal and external systems from an in-house team of specialists, with near real-time triage and response during operational hours.

NRS demonstrate effective security monitoring of their online questionnaire system as part of a managed service. Internal monitoring and response capabilities at **NRS** are maturing.

NISRA will use the online questionnaire system provided by **ONS** and so do not require dedicated monitoring of external systems. Internal monitoring and response capabilities at **NISRA** are maturing.

All Census bodies rely on manual processes for monitoring internal data transfers. Automated monitoring and auditing capabilities have been identified as an opportunity for improvement and work is in progress to ratify requirements at all bodies.

System development

Secure development of a complex system requires robust principles and procedures for the definition of business requirements, technical requirements, success and failure criteria, and then effective implementation to meet those requirements.

All three Census bodies demonstrate operational baseline security controls including vulnerability and patch management, anti-malware, identity and access management, privileged access management and network security.

All three Census bodies maintain separate secured environments for the hosting and processing of Census data, with dedicated workstations and networks isolated from day-to-day environments. Operational and support access to these secured environments is restricted to only authorised individuals with specific business requirements. Privileges, permissions, services, and inbound/outbound access for these secured environments are more restrictively controlled than day-to-day environments. The secured environments within **ONS** and **NISRA** are established. The secured environment within **NRS** is being developed within established infrastructure.

ONS and **NRS** demonstrate a robust set of architectural principles that underpin rigorous design procedures that have been based on multiple areas of industry good practice. Both have defined a comprehensive set of requirements for their respective online questionnaire systems including functional, security, and capacity management. **NISRA** will use key systems provided by **ONS** and so are not directly designing or developing key systems.

ONS and **NRS** have defined a comprehensive set of independent assurance checkpoints for developed systems including IT Health Check, penetration testing, and red team exercises.

Conclusion

The IIAR utilised industry guidance, frameworks and controls, combined with an evidence based assurance approach to ensure objectivity and provide evidence that security activities are designed and operating effectively. Upon consideration of the observed controls, procedures, and governance, the review team are satisfied that citizen data provided in the 2019 Rehearsal and 2021 Census will be appropriately protected against unauthorised access across all three Census bodies, provided development and remediation continues in accordance with their design principles and Bridewell Consulting's recommendations.

Office for National Statistics

NISRA
Northern Ireland Statistics and Research Agency
Gníomhaireacht Thuaisceart Éireann um Staitisticí agus Taighde

National Records of Scotland

Bridewell
CONSULTING

www.bridewellconsulting.com