Australian Census 2016 Online System: A Risk Management Analysis

Riya Patel

Information Systems, Northeastern University

INFO 6245: Planning and Managing Information Systems Development

Professor Shirali Patel

November 14, 2025

Australian Census 2016 Online System: A Risk Management Analysis

The Australian Census in 2016 was a milestone in the Australian Bureau of Statistics' (ABS) aspiration to transition to a "digital-first" approach to the Census process by modernizing data collection, increasing efficiency, and lowering costs. The ABS collaborated with IBM to anticipate that more than 65% of households would submit their Census forms online, a significant increase from 33% in 2011 (MacGibbon, 2016). The ABS, IBM, Australian Signals Directorate (ASD), the Department of the Prime Minister and Cabinet (PM&C), and of course, the Australian public were key stakeholders. Nevertheless, the execution of the project lacked appropriate risk identification processes, insufficient cybersecurity, and communication with stakeholders was inadequate. On Census night (9 August 2016), DDoS attacks occurred, and after a series of attacks the site was shut for 40 hours, leading to the national #CensusFail backlash and trust in government digital initiatives to be significantly eroded (MacGibbon, 2016).

Misapplication of Risk Management Throughout the Lifecycle

The 2016 eCensus indicated serious weaknesses in the execution of risk management processes. While risk matrices and committees were created, the way ABS and IBM functioned underlined mechanisms that embodied compliance rather than proactive mitigation. Cybersecurity was not thought of as an ongoing business risk, but as a technical consideration (MacGibbon, 2016). The ABS had a poorly defined risk appetite, and did not seem to take key risks that are system availability, network resilience, or public perceptions seriously. The risk management plan from IBM incorrectly classified DDoS attacks as "unlikely," which created a false sense of security and limited contingency planning (MacGibbon, 2016). Furthermore, independent testing (IRAP assessment) was not conducted to assess security, which eliminated a key layer of testing that may have revealed approach vulnerabilities in the systems architecture (MacGibbon, 2016).

Cybersecurity, System Performance and Communication Failures

The 2016 eCensus experienced significant failures in both technical and communication aspects. While the possibility of DDoS attacks had been anticipated, the geoblocking plan for "Island Australia" was a flawed plan that was also never tested. IBM did not activate its contract for DDoS protection, and it also misconfigured routers that led to false alarms culminating in the ABS inexplicably shutting down the system (MacGibbon, 2016). At the same time, the ABS did not have a corporate communication and crisis plan in place. For example, information was not quickly disseminated to key stakeholders such as the ABS minister and the PMO, and public updates only indicated the issue as "high traffic" . The ASD was contacted late, leading to less effective coordination across agencies, which delayed action. All of this led to issues with transparency and trust in the public (MacGibbon, 2016).

Implications of Risk Management Failures

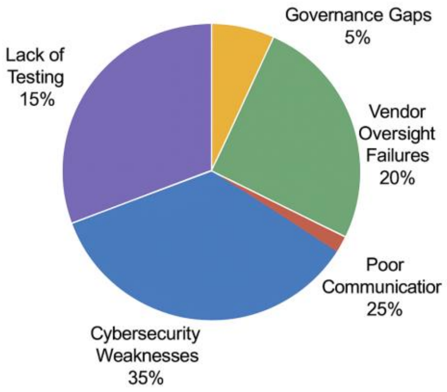
The ABS's credibility and trustworthiness with the public were fundamentally shaken by the cumulative impact of ineffective risk management. While no personal information was compromised as part of the incident, the outage undermined confidence in the government's capacity to protect digital infrastructure. The evidence indicates that there were delayed Census participation and that almost 42% of Australians surveyed conceptualized the Census as a failure (MacGibbon, 2016). The reputational damage extended beyond the ABS, questioning the government's overarching digital transformation agenda at a federal level. The failure also highlighted cultural deficiencies—the ABS was characterized as “insular, inward-looking, and reactive”—that inhibited the capacity to adapt governance and learn from previous deployments in information technology (MacGibbon, 2016).

Impact on Project Outcomes and Public Trust

The 2016 eCensus event caused significant disruption to services and diminished public trust in the Australian Bureau of Statistics (ABS). Significant data collection was halted for more than 40 hours, response times were delayed, and costs of recovery incurred (MacGibbon, 2016). While the system was restored, participation was below expectations and public trust had sharply declined 42% of Australians reported the Census was a failure (ANAO, 2020). There were also increased concerns about data security and privacy. Not surprisingly, the #CensusFail backlash that ensued further damaged the reputation of the ABS. The event ultimately resulted in reforms that influenced the 2021 Census. A stronger reliance on cloud capacity along with layered cybersecurity and improved communication strategies were adopted to facilitate rebuilding public trust (ANAO, 2020).

As illustrated in Figure 1, most of these outcomes stemmed from a combination of cybersecurity weaknesses, poor communication, and vendor oversight failures that collectively undermined the Census's stability and credibility.

Figure 1
Breakdown of Key Risk Failures in the 2016 eCensus



The failure of the 2016 eCensus may have been avoided by a more effective and proactive risk management approach. The success of the delivery of the project and resilience of the system could have been improved through several proactive measures. The main alternative broader options that might have enabled the Australian Bureau of Statistics (ABS) to mitigate at least some of the risks that occurred in the 2016 Census are summarized in Table 1.

Table 1
Alternative Risk Management Strategies for the 2016 eCensus Project

Strategy	Implementation Example	Expected Impact
Independent Risk Assessment	Conduct an IRAP or third-party security review before launch	Identify vulnerabilities early and enable proactive fixes
Layered Cybersecurity & Cloud Resilience	Use ISP-level DDoS protection with multi-region cloud backups	Maintain uptime during attacks and avoid single points of failure
Defined Communication Protocols	Implement a Cyber Incident Response Plan with automated alerts and preapproved messages	Ensure timely crisis communication and maintain public trust
Continuous Monitoring & Testing	Conduct quarterly red-team simulations and update risk registers	Improve preparedness and continuous response capability

Recommendations for Future IT Projects

The 2016 eCensus demonstrated a need for improved integrated risk management practices for large-scale digital projects. To build resilience and develop a more reliable public trust, the following actions can be undertaken in future initiatives:

1. Integrate Risk Management from the Start: Consider risk identification and management as part of the planning. A living risk register would likely have raised the failing “Island Australia” approach before it launched (MacGibbon, 2016).

2. Require Independent Assurance: Require external cybersecurity and operational auditing

before deployment. These independent reviews, similar to what was performed for the 2021 Census, will identify vulnerabilities and help in the matter of accountability (ANAO, 2020).

3. Improve Collaboration and Crisis Management: Formalise the collaboration of the involved agencies, for example ABS, PM&C and ACSC, through the establishment of a national cyber incident response programme with agreed thresholds for escalation and communication (MacGibbon, 2016).

4. Develop a Culture of Accountability: Cultivate a culture of transparency, early escalation of risk, and continuous learning. Ongoing cyber-awareness training and executive “Cyber Bootcamps” can support executive leaders to understand digital risk better (ANAO, 2020).

5. Increase Technical Resiliency: Implement a cloud-first architecture with redundancy and load balancing to avoid creating a single point of failure. The cloud resiliency standards used in the deployment of the 2021 Census should be tasked to inform future digital services (ANAO, 2020).

Together, these strategies embed proactive risk management, improve coordination and ensure government IT systems remain secure, reliable, and publicly trusted.

Conclusion

Using these strategies comprehensive assessment, layered defenses, proactive communication, cloud infrastructures, cultural reform, and ongoing testing would have changed the 2016 eCensus from a reactive project to a resilient project. Each strategy directly addressed a gap identified by MacGibbon (2016) and subsequently confirmed as effective through reforms noted in the 2021 Census (ANAO, 2020). The use of such practices would have developed system stability, ensured public trust, and positioned the ABS as a leader in secure digital governance.

References

Australian National Audit Office. (2020). *Planning for the 2021 Census (Auditor-General Report No. 19 of 2019–20).* Australian Government. https://www.anao.gov.au/work/performance-audit/planning-for-the-2021-census

MacGibbon, A. (2016). *Review of the events surrounding the 2016 eCensus: Improving institutional cybersecurity culture and practices across the Australian government.* Department of the Prime Minister and Cabinet. https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22publications/tabledpapers/a41f4f25-a08e-49a7-9b5f-d2c8af94f5c5%22