Australian Census 2016 Online System: A Risk Management Analysis

Krisha Kaushik Lakhani

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

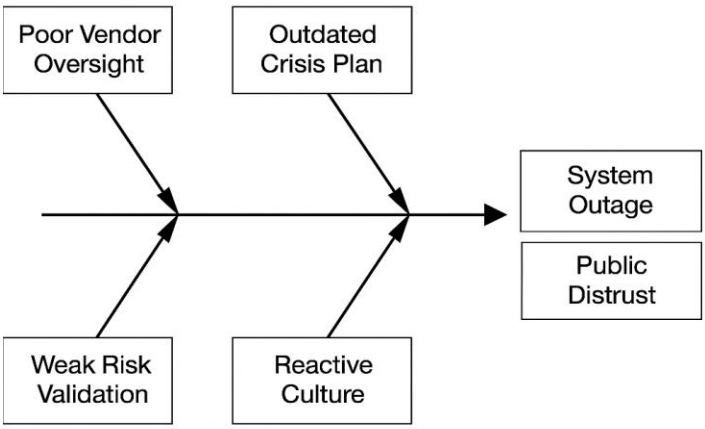
The main objective for the 2016 Australian Census was to adopt a digital-first approach to modernize the way the data was gathered nationwide. To achieve this goal, the Australian Bureau of Statistics (ABS) teamed up with IBM to create the "eCensus" aimed at increasing the efficiency, reducing the expenses, and reaching a 65% online participation rate. The public, the Department of the Prime Minister and Cabinet (PM&C), IBM, the Australian Signals Directorate (ASD), and the ABS were key stakeholders. Unfortunately, a series of Distributed Denial of Service (DDoS) attacks that occurred on August 9, 2016, led to a 40-hour system outage. The #CensusFail was the incident that revealed hospital vendor management, risk identification, and communication, which were major flaws that the local authorities had to deal with (MacGibbon, 2016).

Evaluation of Risk Management Practices

The 2016 eCensus uncovered major deficiencies in risk management. While the ABS recognized cybersecurity threats, it did not check IBM's risk mitigation methods and also lowered the probability of the threat (MacGibbon, 2016). Poor governance and the absence of an IRAP assessment led to vendor lock-in and a loss of opportunities for early problem identification (MacGibbon, 2016). The public was confused due to the delay in the coordination with ministers, the ACSC, and ASD caused by the outdated crisis plans (MacGibbon, 2016; Parliament of Australia, 2016). The ABS's inward and reactive culture, as pointed out by the APSC (2013), was also responsible for the slow responses and over-dependence on IBM.

Figure 1

Root Causes and Consequences of eCensus Risk Management Failures



Note. Based on findings from MacGibbon (2016), APSC (2013), and the Senate Economics References Committee (2016).

Consequences of Risk Management Failures

The eCensus failure led to a 40-hour local time-wide outage that made it impossible for millions of people to complete the online Census. The fact that no data was lost notwithstanding, the event severely affected public trust and the government's online reputation. Surveys show that 33% of Australians thought the data was untrustworthy, and 42% considered the Census a failure (MacGibbon, 2016). It also pointed to the absence of a single, government-wide plan for handling digital risk. The ABS needs to regain its reputation as a reliable data custodian after the Senate Economics References Committee (2016) reported that insufficient communication and governance "deepened a highly avoidable incident that was otherwise obstructed."

Alternative Risk Management Strategies

Independent testing and assessment of security: Potential weaknesses in IBM's "Island Australia" network design and router setup could have been identified through a pre-launch

IRAP review and simulated DDoS tests. Independent verification is necessary for proactive risk management (MacGibbon, 2016).

Cloud resilience and layered cybersecurity: The system would have been always available by using multi-region cloud infrastructure with traffic rerouting and DDoS filtering at the ISP level. The ABS's cautious approach to cloud privacy limited resilience (MacGibbon, 2016).

Defined communication procedures during a crisis: Disorder could have been prevented and public trust regained by a clearly defined Cyber Incident Response Plan that contained the lines of escalation, stakeholder alerts, and social media updates (Parliament of Australia, 2016).

Reforming culture and governance: The ABS had to move from compliance-oriented procedures to a flexible, risk-conscious culture that was open and involved people taking responsibility (APSC, 2013).

Lessons Learned and Recommendations

According to the 2016 eCensus, risk management and cybersecurity should be at the heart of digital government reforms. Organisations ought to:

• Impose the requirement of third-party or independent security reviews (IRAP) for high-risk systems.

• Regularly exercise crisis simulations and conduct stress tests in the case of an attack scenario.

• Through the Cyber Incident Management Arrangements (CIMA), coordinate interagency relations more effectively.

• Building a positive risk climate that focuses on the principles of open communication and the early escalation.

• Employ shared-services cloud security models to secure resilience and scalability.

These changes correspond to the MacGibbon Review recommendation that security should be "baked in" to the design and delivery rather than be an afterthought (MacGibbon, 2016).

Figure 2
Risk Management Lifecycle vs. eCensus Weaknesses

Note. Adapted from PMBOK Guide (6th ed.) and analysis of eCensus findings (MacGibbon, 2016).

Conclusion

The 2016 Australian eCensus was meant to be a landmark in digital modernisation, however, it eventually became a textbook example of how badly the risks were managed. The trouble arose from factors such as complacency, lack of testing, and poor communication, rather than a complex cyberattack. They should consider security and communication as the two most important elements of project governance when they plan new government IT initiatives. Strong risk identification, mitigation, and response measures, among other things, will make it easier to regain trust and ensure that Australia's digital future is both secure and creative.

References

Australian Public Service Commission. (2013). *Capability review: Australian Bureau of Statistics.* https://www.apsc.gov.au/sites/default/files/2021-06/ABS-Capability-Review.pdf

MacGibbon, A. (2016, October 13). *Review of the events surrounding the 2016 eCensus: Improving institutional cyber security culture and practices across the Australian Government.* Department of the Prime Minister and Cabinet. https://apo.org.au/sites/default/files/resource-files/2016-11/apo-nid70705.pdf

Parliament of Australia, Senate Economics References Committee. (2016, November 24). *2016 Census: Issues of trust.* https://apo.org.au/sites/default/files/resource-files/2016-11/apo-nid70704.pdf