The Auditor-General
Auditor-General Report No.34 2025–26
Performance Audit

Cyber Security Readiness for the 2026 Census

Australian Bureau of Statistics

Australian National Audit Office

ISSN 1036–7632 (Print)
ISSN 2203–0352 (Online)
ISBN 978-1-76192-025-7 (Print)
ISBN 978-1-76192-026-4 (Online)

Chief Operating Officer
Corporate Management Group
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Or via email:
communication@anao.gov.au.

Australian National Audit Office

Canberra ACT

27 May 2026

Dear President
Dear Mr Speaker

In accordance with the authority contained in the *Auditor-General Act 1997*, I have undertaken an independent performance audit in the Australian Bureau of Statistics. The report is titled *Cyber Security Readiness for the 2026 Census.* I present the report of this audit to the Parliament.

Following its presentation and receipt, the report will be placed on the Australian National Audit Office's website — http://www.anao.gov.au.

Yours sincerely

Dr Caralee McLiesh PSM
Auditor-General

The Honourable the President of the Senate
The Honourable the Speaker of the House of Representatives
Parliament House
Canberra ACT

AUDITING FOR AUSTRALIA

The Auditor-General is head of the Australian National Audit Office (ANAO). The ANAO assists the Auditor-General to carry out their duties under the *Auditor-General Act 1997* to undertake performance audits, financial statement audits and assurance reviews of Commonwealth public sector bodies and to provide independent reports and advice for the Parliament, the Australian Government and the community. The aim is to improve Commonwealth public sector administration and accountability.

For further information contact:
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Phone: (02) 6203 7300
Email: ag1@anao.gov.au

Auditor-General reports and information about the ANAO are available on our website:
http://www.anao.gov.au

Audit team

James Sheeran
Pam O'Connor
Jeremy Redwin
Margaret Green
Ben Siddans
Susan Drennan

Contents

Audit snapshot

Auditor-General Report No.34 2025–26

Cyber Security Readiness for the 2026 Census

Why did we do this audit?

- The Census is Australia's largest data collection exercise and has followed a digital-first approach since 2016, with a majority of responses submitted online.
- As custodians of highly sensitive citizen-related data, Australian Government entities are expected to operate as cyber exemplars in delivering essential public services.
- An Auditor-General audit of the Australian Bureau of Statistics' (ABS') planning for the 2021 Census concluded that partly appropriate cyber security measures were established and included a recommendation to strengthen Census cyber security.

Key facts

- The Census has been undertaken since 1911 and is conducted every five years.
- On the 2016 Census night, the online form was closed after multiple distributed denial of service (DDoS) attacks and was reopened 40 hours later.
- The 2026 Census will be held on 11 August 2026.

What did we find?

- To be ready for the 2026 Census, the ABS must address key remaining cyber security vulnerabilities by ensuring critical activities will be completed in time.
- There was insufficient consideration to holistic planning for cyber security across the entirety of the ABS ICT environment, which resulted in the delayed identification of cyber security vulnerabilities.
- The ABS monitored 2026 Census cyber security risks but there were shortcomings in completeness and timeliness of risk reviews.
- The Census cyber security assurance program is on schedule, with detection and incident management testing focused on attack vectors identified through threat modelling.

What did we recommend?

- There were four recommendations to the ABS regarding: Census risk management arrangements; early establishment of cyber security advisory arrangements; preparation, approval and review of security architecture documentation; and addressing risks stemming from the broader ABS ICT environment.
- The ABS agreed to the recommendations.

$726 million

The budget for the 2026 Census.

85%

Anticipated online completion rate for the 2026 Census.

1 billion

The approximate number of attempted cyber attacks repelled during the 2021 Census reported by the ABS.

Summary and recommendations

Background

1. Australian Government entities are expected to maintain exemplary cyber security standards because they receive, process and store some of Australia's most sensitive data to support the delivery of essential public services.[1] The 2026 Census is a significant national event with an anticipated online completion rate of 85 per cent, making cyber security readiness across all information and communication technology (ICT) systems supporting the 2026 Census critical.

Audit objective, criteria, and scope

2. The objective of the audit was to assess the readiness of the ABS' cyber security arrangements for the 2026 Census. This audit approach was designed to provide Parliament with timely and targeted assurance of the ABS' cyber security readiness while arrangements are still being implemented ahead of the 2026 Census, enabling findings to inform Census implementation.

3. To form a conclusion against the objective, the ANAO adopted the following criterion:

- Has the ABS designed and implemented controls to mitigate cyber security risks related to the 2026 Census?

4. The audit scope included activities conducted by the ABS to identify, assess and mitigate cyber security risks in readiness for the 2026 Census. It did not include:

- direct testing of, or assurance over, operational effectiveness of the 2026 Census ICT systems' cyber security controls by the ANAO;
- assessment of ABS cyber security arrangements not relating to the 2026 Census; and
- other aspects of the 2026 Census planning and risk management, such as data quality or privacy.

Conclusion

5. To be ready for the 2026 Census, the ABS must address key remaining cyber security vulnerabilities by ensuring critical activities will be completed in time. While the ABS responded quickly and continued to address these vulnerabilities during the audit, this response has required deployment of significant cyber security experts for an extended period beyond that originally anticipated. Earlier consideration of risks across the full ABS ICT environment, incorporating more systematically lessons from Auditor-General Report No. 16 2020–21 *Planning for the 2021 Census*, would have better positioned the ABS to identify and address these issues sooner. Completion of critical cyber security activities is essential to maintaining confidence that Census ICT systems can effectively detect and prevent malicious cyber activity before and during the 2026 Census Main Event.

1 Expert Advisory Board, *2023–2030 Australia Cyber Security Strategy — Discussion Paper*, Home Affairs, Canberra, 2023, p. 19. available from https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf [accessed 24 September 2025].

Supporting findings

Has the ABS identified and assessed cyber security risks related to the 2026 Census?

6. The ABS identified and assessed cyber security risks for the 2026 Census. There were shortcomings in the completeness and timeliness of updates that limited the usefulness of reporting to oversight committees.

- Assessments of related strategic level and program level cyber security risks were not always consistent. Arrangements for assigning responsible officers for risks were not documented and risk owners were not assigned to program level cyber security risks. (See paragraphs 2.9 to 2.11)
- The process for obtaining risk updates was not documented. Prior to July 2025, risk updates were only sought for program risks rated 'high' and above, irrespective of whether they were within target residual severity ratings. (See paragraphs 2.12 to 2.14)
- Oversight committees were not always receiving the most up-to-date or accurate information on cyber security risks. (See paragraph 2.15)

Is there monitoring of Census-related cyber security risks and issues?

7. Oversight committees are monitoring 2026 Census cyber security risks but did not receive timely updates on critical cyber security controls. Gaps in monitoring of Census cyber security risks and assurance began to be addressed through the establishment of the ABS Security Council.

- Oversight committees receive quarterly risk updates to facilitate monitoring of cyber security risks. The Census Program Board only received updates on risks rated 'high' or 'extreme', irrespective of whether the risks were inside of the set tolerance level. Outside of formal risk updates, cyber security risks were included in reporting on the implementation of 2026 Census ICT-related initiatives. (See paragraphs 2.24 to 2.26)
- Risk deep dives conducted in September 2024 and December 2025 found that strategic cyber security risks were likely to be within the set risk tolerance level in time for the 2026 Census. A deep dive was also conducted on the Retrieval Augmented Generation chatbot, which was approved for use in the 2026 Census in December 2025. (See paragraphs 2.27 to 2.28)
- Oversight committees did not receive updates on critical cyber security controls in between strategic risk deep dives, including controls addressing potential sources of risk across the entirety of the ABS ICT environment. (See paragraphs 2.29 to 2.30)
- The ABS Chief Security Officer (CSO) and Chief Information Security Officer (CISO) are both involved in the monitoring of Census cyber security risks through involvement in Census governance committees. The ABS Security Council was created in June 2025 to address gaps in the monitoring of Census cyber security risks and assurance, and support the CSO and CISO in performing their roles. The Security Council's role as an advisory group in the 2026 Census governance structure was formalised in March 2026. (See paragraphs 2.31 to 2.41)
- The ABS' Audit and Risk Committee received briefings on cyber security arrangements for the 2026 Census. (See paragraphs 2.42 to 2.43)

- The ABS is developing arrangements to detect and respond to cyber security incidents. (See paragraphs 2.44 to 2.51)

Is the ABS conducting assurance and testing over cyber security controls?

8. The ABS is conducting assurance and testing over cyber security controls through implementation of the 2026 Census Program Assurance Plan. There are gaps in the delivery of some activities being conducted under the plan. Cyber security detection and incident management arrangements have been tested.

- The ABS established an appropriate program of security testing and assurance activities for the systems that will be utilised in the 2026 Census. Assurance activities and testing are being conducted in line with planned timeframes of the Security Work Program. Gaps were identified in architecture and design reviews. (See paragraphs 2.56 to 2.67)
- Quality gates and gateway-style reviews are designed to provide assurance of quality and compliance. There are gaps in how the quality gates are being monitored and reported. (See paragraphs 2.69 to 2.76)
- Testing for detection and incident management has been conducted based on potential attack vectors identified through threat modelling. Testing confirmed that the monitoring systems are active and identifying issues as they arise, and appropriate procedures were followed through to conclusion of events. (See paragraphs 2.79 to 2.95)

Are there plans in place to address identified issues in cyber security controls in time for the 2026 Census?

9. As at March 2026, plans were in place to address known issues, however, further work is required to identify and address residual vulnerabilities in the ABS ICT environment.

- The ABS established a security uplift plan in November 2025, and actions are being monitored by the ABS Security Council. As at March 2026, plans have been established to address identified issues. The ABS has assigned ‘amber’ ratings to certain actions, and efforts to uplift the broader ABS ICT environment are self-assessed as a ‘medium-high’ risk. (See paragraphs 2.96 to 2.98)
- The ABS gave insufficient consideration to holistic cyber security planning for the 2026 Census as it did not address risks across the entirety of the ABS ICT environment. Similar issues were observed in Auditor-General Report No. 16 2020–21. (See paragraphs 2.99 to 2.107)
- Once the scale of cyber security vulnerabilities affecting preparedness for the 2026 Census became apparent, the ABS quickly identified the need for additional cyber security expertise, which has since been engaged. (See paragraphs 2.108 to 2.109)
- To be ready for the 2026 Census, the ABS must ensure critical activities will be completed in time. (See paragraphs 2.110 to 2.116)

Recommendations

10. The ANAO made four recommendations to the ABS regarding:

- improving risk management arrangements (paragraph 2.16);

- early establishment of cyber security advisory arrangements (paragraph 2.38);
- preparation, approval and review of security architecture documentation (paragraph 2.63); and
- addressing risks stemming from the broader ABS ICT environment (paragraph 2.112).

Summary of entity response

11. The proposed audit report was provided to the ABS. The summary response to the report is below and the full response is at Appendix 1.

Australian Bureau of Statistics

> The ABS continuously reassesses cyber threats and risks, prioritises controls for critical systems, actively adjusts sequencing and investment as vulnerabilities emerge, and integrates planning across Census and non-Census IT systems. The ABS is confident that its multi-layered assurance and continuous reassessment of the threat environment mean we will be ready to deliver the 2026 Census.
>
> The ABS welcomes the recommendations and confirms its commitment to implementing all recommendations in full as part of its focus on continuous improvement. The ABS has adopted a proactive approach, with implementation commencing during the audit period. Actions to address recommendations one and two have been completed, and substantial progress has been made against recommendations three and four. This work ensures the ABS is well positioned and operationally prepared for the 2026 Census.
>
> The ABS will continue to prioritise these improvements and allocate appropriate resources to support their successful delivery. This commitment extends beyond readiness for the 2026 Census, to also strengthen the quality, efficiency and resilience of future Censuses.

Key messages from this audit for all Australian Government entities

12. Below is a summary of key messages, including instances of good practice, which have been identified in this audit and may be relevant for the operations of other Australian Government entities.

Governance and risk management

- Clear documentation of how responsible officers are assigned to risks underpins accountability and helps ensure risks are actively owned, monitored and managed.
- Timely, accurate and meaningful reporting on the implementation and effectiveness of controls is critical to enabling senior leaders and governing bodies to support effective oversight of risks and emerging issues.
- Embedding subject matter expertise in governance arrangements strengthens assurance by ensuring senior officials receive clear, reliable and technically informed advice to support risk-based decision making.
- When an entity receives recommendations from a parliamentary committee or the Auditor-General, it is essential to consider their relevance beyond the immediate scope of the review. Applying recommendations to related projects, programs and business areas reflects a mature, risk-based approach and helps reduce the likelihood of issues recurring.

Policy/program implementation

- Entities should formally capture lessons learnt and implementation challenges from prior initiatives, including from audits, reviews and post-implementation assessments.
- Lessons learnt should be embedded into future planning, governance, and risk frameworks rather than treated as one-off responses to specific events. Doing so supports continuous improvement and strengthens an entity's resilience over time.

Audit findings

1. Background

Introduction

The next Census of Population and Housing is scheduled for 11 August 2026.

1.1 The Census of Population and Housing (the Census), Australia's largest data collection exercise, is conducted by the Australian Bureau of Statistics (ABS). It provides essential information for public policy development, determining funding for different levels of government, electoral boundary setting and supporting research on Australia's economic, social and cultural make up.

1.2 Under subsection 8(1) of the *Census and Statistics Act 1905,* the Census is required to occur every five years. The most recent Census was held on 10 August 2021 and the next Census is scheduled for 11 August 2026.[2] For both the 2021 and 2026 Censuses, the ABS has established a 'response window', beginning when households receive the Census form, for people to complete the Census, with the specific Census date providing the reference point for responses when answering Census questions.

1.3 The ABS' budget for delivering the 2026 Census is $726 million across the period 2022–23 to 2026–27. The overall budget is an increase from the 2021 Census, which had a budget of $577 million. The ABS will temporarily hire more than 30,000 people to assist with undertaking the 2026 Census.

1.4 The 2026 Census has three objectives, which are the same objectives as those for the 2021 Census:

1. Smooth running – the Census experience is easy, simple and secure
2. Strong support – governments, businesses and the community have confidence in the Census and there is a high level of community participation
3. High quality data – Census data is high quality and widely used to inform on areas of importance to Australia.

Census cyber security

1.5 Cyber security is a key risk to the successful delivery of the Census. The 2016 Census was Australia's first predominantly digital Census, with the ABS setting a target of 65 per cent of responses being completed through an online 'eCensus' form.[3] On Census night, the online Census form was closed after multiple distributed denial of service (DDoS) attacks[4], and subsequently reopened 40 hours later. This event prompted several reviews into the ABS' cyber security measures, including a parliamentary inquiry[5] and a review by the Special Adviser to the

2 The first Census was held in 1911. The 2026 Census will be the 19th Census.

3 The online completion rate for the 2016 Census was 58.8 per cent. In the 2006 and 2011 Censuses, the ABS provided Australian households with a paper form as well as the option of entering data online.

4 A DDoS attack overloads a network with so much malicious traffic that it cannot operate or communicate as it normally would.

5 Senate Economic References Committee, *2016 Census: issues of trust*, Parliament of Australia, Canberra, 2016, available from https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Economics/2016Census/Report [accessed 18 May 2026].

Prime Minister on Cyber Security.[6] In November 2016 the Australian Government reached a confidential settlement with IBM, which had been contracted to deliver the online Census capability.

1.6 Auditor-General Report No.16 2020–21 *Planning for the 2021 Census* found that cyber security measures for the 2021 Census were 'partly appropriate' and included a recommendation aimed at strengthening Census cyber security.[7] The ABS reported that during the 2021 Census it 'repelled almost 1 billion attempted cyber-attacks, and we also blocked 130,000 malicious IP (network) addresses.'[8] In June 2023, the ABS prepared a Program Closure Report for the Senior Responsible Officer for the 2021 Census that included reflections on achievement of objectives and lessons learnt for future Censuses, including relating to Census cyber security.

Preparations for the 2026 Census

As a custodian of sensitive citizen-related data, the ABS is expected to operate as a cyber exemplar in delivering the 2026 Census.

1.7 The ABS commenced preparations for the 2026 Census in December 2021 with its work program divided into five tranches. Figure 1.1 outlines the timeline for preparations.

6 Alastair MacGibbon, *Review of the Events Surrounding the 2016 eCensus*, PM&C, Canberra, 2016, available from https://parlinfo.aph.gov.au/parlInfo/download/publications/tabledpapers/a41f4f25-a08e-49a7-9b5f-d2c8af94f5c5/upload_pdf/Review%20of%20the%202016%20eCensus%20-%20final%20report.pdf [accessed 18 May 2026].

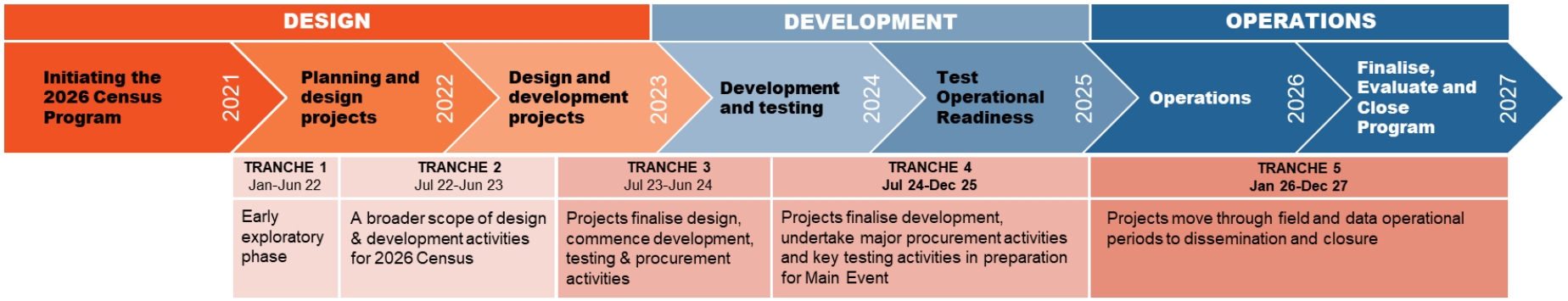
7 Auditor-General Report No.16 2020–21, *Planning for the 2021 Census,* available from: https://www.anao.gov.au/work/performance-audit/planning-for-the-2021-census [accessed 16 December 2025].
Recommendation 5 in Auditor-General Report No.16 2020–21 was that:

> The Australian Bureau of Statistics:
>
> a. define timeframes and responsibilities for implementing the 2021 Census Security Strategy and the Essential Eight Uplift Program, especially for areas that are required prior to the 2021 Census; and
>
> b. ensure contracted services meet Australian Bureau of Statistics specific design and cyber security requirements, and performance of security controls are regularly assessed.

ABS documentation indicates that the recommendation was implemented in April 2021.

8 Australian Bureau of Statistics, *Delivering the 2021 Census: Story 4: Security and privacy by design*, ABS, Canberra, 10 August 2022, available from https://www.abs.gov.au/census/about-census/delivering-2021-census/story-4-security-and-privacy-design#:~:text=During%20the%20Collection%20period%20when%20the%20Census,also%20blocked%20130%2C000%20malicious%20IP%20(network)%20addresses. [accessed 23 September 2025].

Figure 1.1: Timeline of preparations for the 2026 Census



Source: ABS documentation.

1.8 In August 2025, a key milestone completed as part of the 2026 Census preparation was an Operational Readiness Exercise (ORE), also referred to as a Census Test. The ORE tested collection processes and ICT systems across a sample of 51,752 dwellings and 9,803 respondents through the myGov[9] platform.

1.9 In August 2024, the Australian Statistician announced that an additional earlier Census Test planned for 2024 would not proceed due to an Australian Government announcement that Census topics would not be changed from those used in the 2021 Census.[10] In September 2024, the Australian Government announced that a new topic of 'sexual orientation and gender' would be included in the 2026 Census.[11] The topic was subsequently included in testing conducted as part of the ORE. The 2024 Census Test formed part of the ABS' quality gate schedule under the 2026 Census Program Assurance Plan (see paragraphs 2.70 to 2.74).

2026 Census governance arrangements

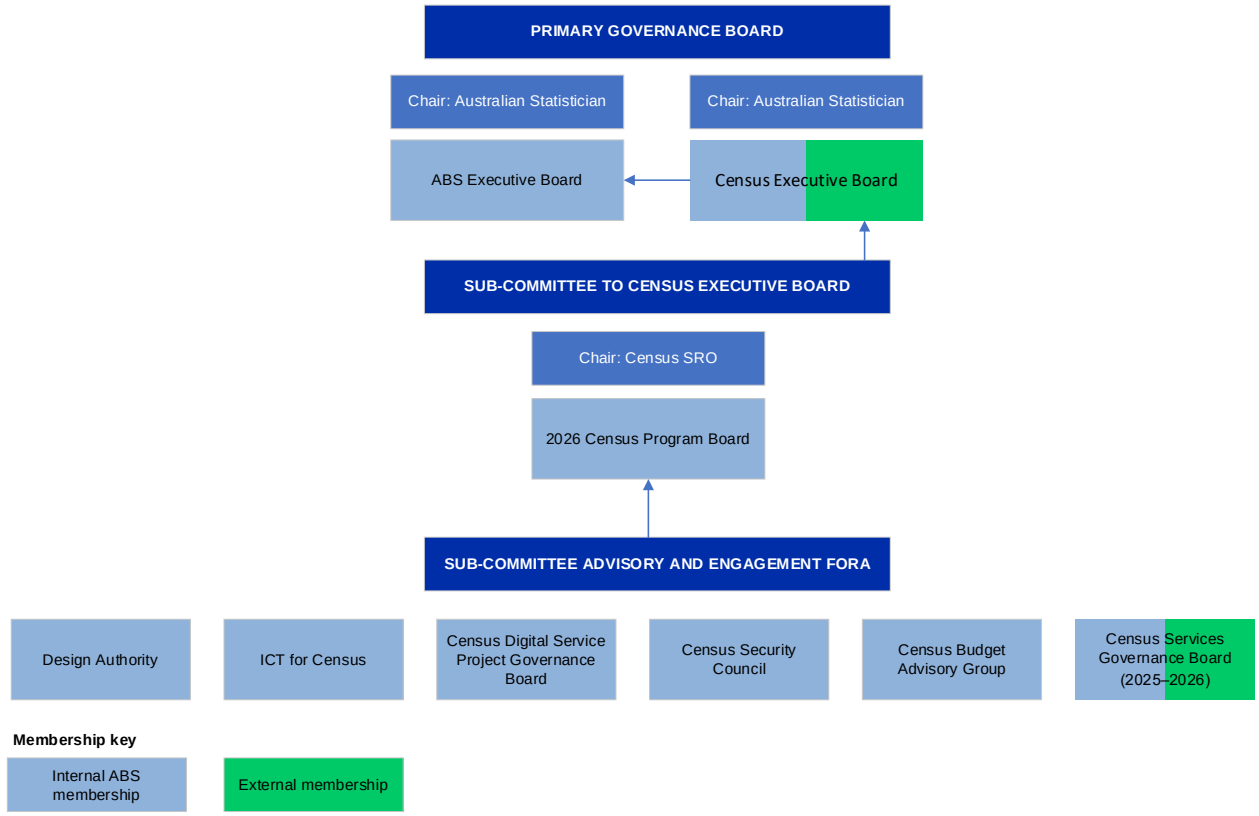
1.10 In September 2022, the ABS developed the 2026 Census Program: High-level Governance Plan, which outlines the governance responsibilities and management principles supporting the preparation for the 2026 Census. The plan identifies the Senior Responsible Officer (SRO) as the person 'accountable for overall design and delivery' of the 2026 Census. The SRO position is held by the Deputy Australian Statistician — Insights and Statistics Group who is 'responsible for major decisions, operations, and outcomes for the 2026 Census Program.' This role operates within a broader governance structure outlined in Figure 1.2.

9 The myGov digital platform is used for accessing a broad range of Australian Government services. ABS documentation states that myGov is to be an 'entry point' for the 2026 Census and 'individual household data will not be stored or available to myGov.'

10 The Census consists of topics determined by the Australian Government and the Parliament. Topics are included in the Census and Statistics Regulation 2016, with the ABS responsible for determining the wording and layout of questions under each topic.

11 Assistant Minister for Competition, Charities and Treasury, 'New topic in the 2026 Census', media release, 8 September 2024, available from https://ministers.treasury.gov.au/ministers/andrew-leigh-2022/media-releases/new-topic-2026-census [accessed 10 March 2026].

Figure 1.2: 2026 Census Program Governance Structure



Source: ABS documentation.

1.11 The primary oversight committee for the 2026 Census is the Census Executive Board (CEB), which meets quarterly. This board is chaired by the Australian Statistician (the ABS' accountable authority) and oversees 'the strategic direction of the Program and the achievement of the 2026 Census objectives'. In addition to the chair, the CEB comprises:

- three Deputy Australian Statisticians, including the SRO[12]; and
- six 'external members' from the public and private sectors.[13]

1.12 The 2026 Census Program Board (CPB) is a subcommittee that reports to the CEB. It meets quarterly and is chaired by the SRO. The CPB was established to 'monitor and assure the delivery of the Program, support key decision making and advise the SRO'. Delivery of the 2026 Census is further supported by subcommittees that report to the CPB, with the Census Program Management Office providing central coordination support.

12 Collectively, the Australian Statistician and the three Deputy Australian Statisticians comprise the ABS' Executive Group.
Australian Bureau of Statistics, *Organisation Chart*, ABS, Canberra, December 2025, available from https://www.abs.gov.au/about/our-organisation/organisation-chart [accessed 9 December 2025].

13 External members include senior personnel from Services Australia, the Australian Electoral Commission, the New South Wales Cabinet Office, Statistics Canada, CyberCX and Telstra. In selecting external CEB members for the 2026 Census, the ABS sought to retain members with previous Census experience and add members with 'experience in designing large complex programs with a substantial IT component.'

1.13 The ABS has engaged with the Department of the Treasury (Treasury), its portfolio department[14], as part of the 2026 Census preparations, including seeking advice on legislative and budgetary matters. Both the ABS and Treasury are represented on the Australian Statistics Advisory Council where the ABS has also briefed on preparations for the 2026 Census.[15]

1.14 After each CEB meeting, the SRO provides an update to the Assistant Minister for Competition, Charities and Treasury.[16] This practice was established in response to a recommendation included in the Senate Economics References Committee *2016 Census: issues of trust* report.[17] Updates included information on: the overall Census Program status; outcomes of key assurance activities; outcomes of strategic level risk deep dives; Census budget management; preparations for and outcomes of the ORE; and the planned approach for privacy management, data dissemination and the use of AI. The Treasurer and the Secretary to the Treasury were included in the Census program updates.

2026 Census Information and Communication Technology (ICT) systems

Eighty-five per cent of Australians are expected to complete the 2026 Census form online.

1.15 The 2026 Census Program Strategy developed by the ABS states that: 'The 2026 Census will reuse most of the 2021 Census model with carefully considered innovation to address risk and optimise key aspects of design and operation.' Key ICT systems from the 2021 Census will also be reused for the 2026 Census. This includes the Census Digital Service (CDS), which hosts the online Census form that most households will complete on Census night, and systems used to facilitate data collection.[18] Processing and coding systems were largely redeveloped for the 2026 Census to replace aging components and uplift the security posture of these systems.[19] In January 2024, the ABS announced Slalom Australia and Amazon Web Services (AWS) would be its ICT partners for

14 While the ABS is independent and accountable for delivery of the Census, information sharing with the portfolio department assists the Secretary to the Treasury in performing duties under the Secretaries Performance Framework relating to leading implementation of programs across their portfolios.
Department of the Prime Minister and Cabinet, *Secretaries Performance Framework*, PMC, 2025, available from https://www.pmc.gov.au/resources/secretaries-performance-framework [accessed 11 March 2026].

15 This council is not part of the 2026 Census Governance Structure outlined in Figure 1.2. Established under the *Australian Bureau of Statistics Act*, the Australian Statistics Advisory Council is:

> the key advisory body to the Minister and the Australian Bureau of Statistics (ABS) on statistical services. This includes addressing the priority of maintaining and enhancing the quality of official statistics, as well as providing valuable input to the directions and priorities of the ABS work program.

Australian Bureau of Statistics, *Australian Statistics Advisory Council*, ABS, Canberra, available from https://www.abs.gov.au/about/legislation-and-policy/australian-statistics-advisory-council [accessed 15 January 2026].

16 The Minister was provided with an update following the eight CEB meetings between January 2024 and December 2025.

17 Recommendation 11 was that:

> The committee recommends responsible ministers seek six-monthly briefings on the progress of census preparations. These briefings should cover issues including, but not limited to, cyber security, system redundancy, procurement processes and the capacity of the ABS to manage risks associated with the census.

Senate Economics References Committee, *Report: 2016 Census: issues of trust*, p. 72.

18 These include systems relating to management of the temporary Census workforce and field operations undertaken for the Census.

19 Processing and coding systems used in 2021 Census were originally developed for the 2006 Census and designed around paper-based census forms.

delivery of digital services for the 2026 Census.[20] The ABS is also receiving support and assistance for the 2026 Census from the Australian Cyber Security Centre and other cyber security experts.

1.16 Census ICT systems are approved by the ABS' Chief Security Officer through an 'Authority to Operate' process. This process is required by the Protective Security Policy Framework (PSPF)[21] and is intended to ensure that appropriate security is applied to a system and residual risks have been accepted by the relevant authority.[22]

1.17 The ABS anticipates that 85 per cent of 2026 Census forms will be completed online, which would be an increase from the 58.8 per cent online completion rate for the 2016 Census and 78.9 per cent for the 2021 Census. For the first time, the 2026 Census will be accessible through myGov.[23] The ABS is utilising artificial intelligence (AI) to 'enhance customer experience' and for processing responses contained within the Census forms.[24] The Census website will feature 'a Retrieval Augmented Generation (RAG) chatbot' designed to answer website users' questions.[25] Hardcopy Census forms will remain available. The ABS provides additional support for people who need it, including people living with disability, people experiencing homelessness and migrants, refugees and international visitors.[26]

1.18 Under the Whole of Government Digital and Information Communications Technology (ICT) Investment Oversight Framework, the Digital Transformation Agency (DTA) supports Australian Government entities to manage its digital and ICT enabled investments.[27] The 2026 Census is designated by the DTA as a Tier 2 Strategically Significant Digital Investment, which requires entities to provide the DTA with annual updates on assurance plans (see paragraph 2.53), biannual delivery

---

20 The Census Digital Service is hosted using Amazon Web Services Cloud.
Australian Bureau of Statistics, 'ABS partnering with Slalom Australia to deliver the 2026 Census Digital Services', media release, 24 January 2024.
As of December 2025, the value reported on AusTender of the ABS' contract with Slalom Australia was $36 million and the total value of the ABS' contracts with Amazon Web Services was $5.46 million.

21 The PSPF 'sets out Australian Government policy across six security domains and prescribes what Australian Government entities must do to protect their people, information and resources, both domestically and internationally'. The six security domains defined in the PSPF are: governance; risk; information; technology; personnel; and physical. Domains are not mutually exclusive.
Department of Home Affairs (DHA), *PSPF Annual Release 2025*, DHA, Canberra, 24 July 2025, available from https://www.protectivesecurity.gov.au/publications-library/pspf-annual-release-2025 [accessed 30 January 2026].

22 The standards are set out in section 13.3 of DHA, *PSPF Annual Release 2025*, p. 62.

23 See Footnote 9 for an explanation of myGov.

24 The ABS advised in May 2026 that:

> The ABS is using Machine Learning models to code written responses provided on Census forms. These models will be used to code written responses to Occupation, Industry, Education, Religion, Ancestry, Language and Country of Birth questions to the relevant classification. All data used to train and run these models is securely stored and processed within ABS systems.

Also see: Australian Bureau of Statistics, *AI transparency statement*, ABS, Canberra, available from https://www.abs.gov.au/about/legislation-and-policy/ai-transparency-statement [accessed 14 May 2026].

25 Chatbots are computer programs that simulate human conversations. The chatbot hosted on the ABS website for the 2021 Census could only answer predefined questions. A Retrieval Augmented Generation chatbot is an AI conversational agent that retrieves real-time data from authorised knowledge bases, such as company documents, FAQs, or databases, before generating a response.

26 Australian Bureau of Statistics, *Help and support*, ABS, Canberra, 2026, available from https://info.census.abs.gov.au/help [accessed 14 May 2026].

27 Digital Transformation Agency, *Digital and ICT Investment Oversight Framework*, Australian Government, Canberra, available from https://www.digital.gov.au/investment [accessed 12 January 2026].

confidence assessments and final assurance reports. Project Collection Survey Forms (also known as 'wave reports') have been completed quarterly by the ABS since October 2024, as required by the DTA, and include reporting on delivery confidence assessments. The ABS is also engaging with the DTA on the implementation of the Digital Experience Policy for the 2026 Census.[28]

Audit methodology

1.19 The audit methodology involved:

- reviewing cyber security risk identification, assessment and monitoring relating to cyber security for the 2026 Census;
- reviewing ABS cyber security plans and strategies for the 2026 Census and reviewing testing of cyber security controls conducted by, or on the behalf of, the ABS; and
- meeting with key personnel involved in the preparation for the 2026 Census and cyber security testing.

1.20 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of approximately $447,882.

1.21 The team members for this audit were James Sheeran, Pam O'Connor, Jeremy Redwin, Margaret Green, Ben Siddans, and Susan Drennan.

28 The Digital Experience Policy 'sets agreed benchmarks for high-quality digital service design and supports a whole-of-government approach to improving how people and business interact digitally with government information and services.' It applies to investments subject to the ICT Investment Oversight Framework. Digital Transformation Agency, *Digital Experience Policy*, DTA Canberra, available from https://www.digital.gov.au/policy/digital-experience [accessed 15 January 2026].

2. Controls to mitigate cyber security risks

Has the ABS identified and assessed cyber security risks related to the 2026 Census?

2026 Census risk management approach

2.1 The ABS sets outs how it will manage risks and issues for the 2026 Census in the 2026 Census Program Risk and Issues Management Plan (RIMP). The RIMP states that the approach to risk management 'aligns with the ABS Risk Management Framework and Commonwealth Risk Management Policy[29], and draws from relevant ABS and Commonwealth Guidance and contemporary best practice'.

2.2 As was the case with the 2021 Census, the RIMP establishes a three-tiered approach to the oversight and management of risks for the 2026 Census. Table 2.1 outlines the three-tiered approach.

Table 2.1 2026 Census risk categories

Risk category	Description	Reported to
Strategic level risks	Risks that are most closely aligned with ABS strategic risks or have the greatest potential to significantly harm the ABS.	Census Executive Board
Program level risks	Includes the most material operational concerns that could jeopardise the success of the Census.	Census Program Board
Project level risks	The most granular risks and are defined against the objectives of each project conducted for the 2026 Census.	Census Program Management Office

Source: ABS Documentation.

2.3 Overall responsibility for risks and issues management in the implementation of the 2026 Census resides with the Senior Responsible Officer (SRO), which is the Deputy Statistician. The Census Program Management Office (CPMO) provides central coordination and support for risk management activities.

2.4 The RIMP sets the parameters for the 2026 Census risk appetite statement, which outlines the level of risk the ABS is willing to accept in delivering the 2026 Census.[30] Strategic and program level risks are captured in a centrally managed risk register, which includes information on:

29 The Commonwealth Risk Management Policy, first established in 2014 and updated in November 2022, aims to 'embed risk management into the culture and work practices of [Australian Government] entities to improve decision making in order to maximise opportunities and better manage uncertainty' Department of Finance, *Commonwealth Risk Management Policy* [Internet], Finance, Canberra, 2022, available from https://www.finance.gov.au/government/comcover/risk-services/management/commonwealth-risk-management-policy [accessed 8 December 2025].

30 The risk appetite statement 'describes the amount and type of risk the ABS is prepared to accept in achieving the 2026 Census Program's strategic objectives of 'Smooth Running', 'Strong Support' and 'High Quality Data'.'

- 'inherent', 'residual' and 'target' risk ratings[31], which are assessed as either 'low', 'medium', 'high' or 'extreme' in accordance with the ABS' defined likelihood/consequence matrix;
- identified causes and potential consequences of each risk;
- designated responsible officers[32];
- controls to mitigate the risks (preventative, detective and mitigation/recovery);
- control effectiveness ratings;
- the status of residual risk severity (rated as 'low', 'medium', 'high' or 'extreme'), and further indicating whether it is 'Acceptable', 'Under Treatment' or 'Escalation Required'; and
- 'proximity date', which indicates the date a risk could be realised, informing the timeframe available to implement risk treatments.

2.5 Project level risk registers are developed and maintained by project managers and are not managed centrally.

Identification and assessment of cyber security risks

The ABS documented the identification and assessment of cyber security risks for the 2026 Census.

2.6 The 2026 Census risk appetite statement was first endorsed by the Census Program Board (CPB) in October 2022. It stated that 'The 2026 Census has a low risk appetite for breach or compromise from attack' and 'a low risk appetite for the loss of availability of the online form due to a cyber-attack or other system failure during the enumeration period.' The statement was revised in September 2025 following a review of risk management arrangements (see paragraph 2.21). The revised risk appetite statement stated that:

> The Census Program has limited appetite for privacy and information security risks, recognising not all such risks can be reduced to a 'Low' severity level despite taking all reasonably practicable measures and complying with legal and regulatory requirements.

2.7 There was one strategic level risk and two program level risks directly relating to cyber security.

- **Strategic level risk 5 (SR5)**: 'The ABS is unable to, or is perceived to be unable to, protect Census data, including against cyber threats.'
- **Program level risk 3 (PR3)**: 'Census customer facing systems are unavailable or unable to effectively mitigate cyber attacks.'
- **Program level risk 6 (PR6)**: 'The Census is unable to, or perceived to be unable to, protect 2026 Census data.'

2.8 Table 2.2 outlines how the ABS' assessment of these risks changed over the period between January 2024 and March 2026, with further information at paragraph 2.9.

31 'Inherent' risk is the level of risk that exists before controls or treatments are considered. 'Residual' risk exists after controls and treatments have been applied. 'Target' ratings reflect the desired severity of the risk.

32 Prior to December 2025 this was the 'primary program lead'. From January 2026 this was changed to 'risk lead'. Risk owners were not documented in the register.

Table 2.2 ABS assessment of 2026 Census strategic and program level cyber security risks, January 2024 to March 2026

Risk ID	Risk category	Risk description	Inherent severity[a]	Residual severity	Target severity	Control effectiveness[b]	Proximity date[c]
SR5	Strategic level risk	The ABS is unable to, or is perceived to be unable to, protect Census data, including against cyber threats.	Extreme	**High**	**Low** (January 2024 to October 2025) **Medium** (November 2025 onwards)	**Substantially effective** (October 2024 onwards)	**August 2026** (January to August 2024) **March 2026** (October 2024 to February 2025) **August 2025**[d] (February to November 2025) **Q1 2026** (November 2025 onwards)
PR3	Program level risk	Census customer facing systems are unavailable or unable to effectively mitigate cyber attacks.	High	**Medium** (January 2024 to April 2025, October 2025 onwards) **High** (July to August 2025)	**Low** (January 2024 to August 2025) **Medium** (October 2025 onwards)	**Substantially effective** (January 2024 to April 2025, October 2025 onwards) **Partially effective** (July to August 2025)	**December 2026** (October 2025 onwards)
PR6		The Census is unable to, or perceived to be unable to, protect 2026 Census data.	Extreme	**High**	**Low** (January 2024 to October 2025) **Medium** (November 2025 onwards)	**Substantially effective** (April 2025 onwards)	**August 2026** (April to November 2025) **Q1 2026** (December 2025 onwards)

Note a: Inherent severity was recorded from May 2024 onwards.

Note b: Control effectiveness is determined in the Strategic and Program Risks Register by the risk lead for each risk as they review and update their risk assessment. The risk register did not contain information on control effectiveness for SR5 until October 2024 or PR6 until April 2025.

Note c: Proximity date indicates the date a risk could be realised, informing the timeframe available to implement risk treatments. The risk register did not contain information on proximity date before October 2025 for PR3 and April 2025 for PR6.

Note d: This was to align with the Operational Readiness Exercise (ORE), which was held in August 2025.

Source: ANAO analysis of ABS documentation.

Assessments of related strategic level and program level cyber security risks were not always consistent.

2.9 While PR3 and PR6 overlap with SR5, they are monitored and reported on separately. Changes in assessments for strategic level risks do not automatically flow through to program level risks, and vice-versa. For example, proximity dates were often inconsistent between the program level cyber security risks and SR5. Key information that was present in the registers for some cyber security risks was missing for others, including: control effectiveness ratings (for SR5 until October 2024 and PR6 until April 2025) and proximity dates (for PR3 until October 2025 and PR6 until April 2025). The separation of monitoring and reporting of overlapping risks could create inefficiencies and limit decision-makers' access to current assessments of risks and required actions to mitigate them.

Responsible officers

Arrangements for assigning responsible officers for risks were not documented and risk owners were not assigned to program level cyber security risks.

2.10 Clarity of risk management roles and responsibilities is essential for effective risk management. The RIMP defines the role of 'Risk/Issue Owners', which is a term that does not appear in the ABS' 2026 Census strategic and program risk registers. In January 2026, the RIMP was updated to also include the role of 'Risk Lead'. The RIMP provides no criteria or guidance on the seniority or specialist expertise required for assigning a responsible officer to a risk.

2.11 Prior to December 2025, the risk register included a 'Primary Program Lead' for each risk, a role that was not defined in the RIMP. This title was updated to 'Risk Lead' to reflect the January 2026 revision of the RIMP. Between January 2024 and December 2025, the Director of the Program Management Office was assigned as the Primary Program Lead for SR5 and PR6 and the Primary Program Lead for PR3 was the Director, Census Digital Service.[33] A subsequent decision was made by the ABS for the December 2025 strategic level risk deep dive (see paragraph 2.27) that assigned the 'risk owner' for SR5 as the General Manager, Census & Population Division and the 'risk leader' as the Chief Information Security officer. Risk owners for PR3 and PR6 are not documented, despite these risks being reported to the Census Program Board. These arrangements contributed to weaknesses in risk governance for critical cyber security risks.

Risk reassessments

The process for obtaining risk updates was not documented. Prior to July 2025, risk updates were only sought for program risks rated 'high' and above, irrespective of whether they were within target residual severity ratings.

2.12 Under the RIMP, strategic and program level risks are required to be reviewed and updates prepared for meetings of the respective oversight committees (see Table 2.1). There are no documented procedures for the timing of updates or level of detail to be included.

2.13 The ABS advised the ANAO in January 2026 that the Census PMO 'began seeking written strategic-level and program-level risk updates from risk leads via email in June 2024. Prior to this,

33 Prior to May 2024, the Director Census Technology & Security Division was also listed as a Primary Program Lead for PR3.

updates were provided verbally by risk leads and recorded in meeting notes in minimal detail.' From February 2025, primary program leads were requested to complete a standardised template that prompted a review of risk severity, control effectiveness, acceptability and proximity. The ABS advised the ANAO in November 2025 that control effectiveness is assessed by risk leads and control owners with consideration given to:

- the main challenge/s to reducing this risk to within appetite
- the most critical gaps and weaknesses in the controls
- the main actions being taken to address the challenges, gaps and weaknesses, and reduce the risk to within appetite
- any significant changes since the previous review, that affect our ability to manage this risk (E.g., changes in operating context, causal factors, effectiveness of critical controls)

2.14 From June 2024, updates for SR5 and PR6 were sought quarterly. Between June 2024 and March 2026, SR5 and PR6 were both reviewed seven times. Updates on PR3 were sought only three times in the same period. ABS documentation indicates that prior to July 2025, the CPMO sought updates from primary program leads only on program level risks rated 'high' and above, irrespective of whether risks were within target residual severity ratings. When this practice was expanded to include medium-rated risks, PR3's residual severity rating was temporarily raised to 'high' as a result of reassessment.

Oversight committees were not always receiving the most up-to-date or accurate information on cyber security risks.

2.15 Risk updates are collated by the CPMO and inform reporting to the Census Executive Board and Census Program Board (see paragraphs 2.24 and 2.25). A total of 17 risk updates were requested by the CPMO for SR5, PR3 and PR6 between June 2024 and March 2026.

- **Three (18 per cent) had no documented response**: This meant there was no documented consideration of key factors such as residual risk severity and control effectiveness to inform reporting to oversight committees.
- **Six (35 per cent) included updates on the cyber security components of the risk**: Where there was no cyber security update, the documentation either referred to the privacy component of the risk (applicable to SR5 and PR6) or stated that there was no change from the previous update without any documented reflection on progress towards strengthening cyber security controls.
- **Updates were not current**: Where there were documented updates, they were completed an average of 31 days prior to the oversight committee meeting at which the risks were reported. This means oversight committees were not always receiving the most up-to-date information on cyber security risks.

Recommendation no. 1

2.16 The Australian Bureau of Statistics strengthen its Census risk management arrangements by:

(a) clearly linking strategic and program level risks, particularly where they overlap;

(b) documenting the arrangements for assigning responsible officers to risks; and

(c) establishing documented processes for the timing and the content of risk updates by responsible officers.

Australian Bureau of Statistics response: *Agreed.*

2.17 *The ABS recognises the importance of strong risk management. The ABS is continuously enhancing and evolving its approach to strengthen risk management. From mid-2025 onwards, the Census Program's risk management focus shifted increasingly from strategic to operational. The Program commenced regular updates each reporting period on all strategic and program level risks, using a structured format.*

2.18 *The Census Program has analysed overlaps in strategic and program level risks, to ensure they are being managed effectively and consistently. Where overlaps exist and the risk leads for the overlapping risks are not the same, additional measures have been taken to ensure the management and alignment of these risks are well-integrated and consistent.*

2.19 *The ABS continuously reassesses threats and risks and actively manages risks by prioritising controls to ensure risk mitigation. Building on the ABS' existing risk management approach, the ABS has strengthened its processes including development of documentation to outline the process for assigning responsible officers to risk as well as clearly outlining the process of structured, regular risk updates.*

2.20 *These changes address opportunities for improvement for the 2026 Census identified during the audit.*

Reviews of 2026 Census risk management arrangements

2.21 In August 2024, a Specialist Review conducted as part of the 2026 Census Program Assurance Plan (see paragraphs 2.52 to 2.78) concluded that across the 2026 Census program risks were:

> being actively managed through the involvement and culture of [Census] Program staff at all levels. Some minor improvements in capability and realignments of artefacts and processes will ensure this is fully effective and suited to the evolving needs of the Program as it moves through its life cycle into 2026.

The review recommended a refresh of the 2026 Census risk appetite statement, which had not been updated since October 2022. This was subsequently updated in September 2025.

2.22 As part of the 2026 Census Security Work Program, a security audit was conducted by a contracted supplier for the period between May and July 2025, with the final report being provided to the ABS in October 2025. The review was to 'examine the security assurance and governance processes supporting the Census, with a view to ensuring appropriate rigour was being applied to security for the Census'. The review found that a lack of integration with the ABS' Security and Information Assurance Branch was 'impacting the visibility of security considerations in decision-making, delaying or reducing the accuracy of risk assessments, and contributing to some inconsistency in approval processes'. The review made two recommendations relating to risk management, which were that the ABS:

> Increase the resourcing and or allocation of effort provided from SIA [Security and Information Assurance Branch] in providing external assurance of the Census Program ...
>
> Uplift the level of detail currently presented in security risk mitigation and treatment registers … [including] that the risk register be enhanced to include clearer status indicators, responsible parties, and due dates for mitigation actions.

2.23 The ABS agreed to the recommendations, with the first of the recommendations outlined above being implemented in October 2025, including through the establishment of the ABS Security Council (see paragraphs 2.35 to 2.41). The ABS advised the ANAO in January 2026 that implementation of the second recommendation was ongoing.

Is there monitoring of Census-related cyber security risks and issues?

Risk reporting to oversight committees

Oversight committees receive quarterly risk updates to facilitate monitoring of cyber security risks. The Census Program Board only received updates on risks rated 'high' or 'extreme', irrespective of whether the risks were inside of the set tolerance level. Outside of formal risk updates, cyber security risks were included in reporting on the implementation of 2026 Census ICT-related initiatives.

2.24 The 2026 Census governance arrangements include oversight by the Census Executive Board (CEB), chaired by the ABS accountable authority, and the Census Program Board (CPB), chaired by the 2026 Census SRO. Both the CEB and CPB receive dashboards at each meeting containing information on risks in the strategic and program risk register.

- The CEB received updates on all strategic level risks (including SR5) that included information on: risk severity (inherent, residual and target); control effectiveness ratings; risk acceptability; and proximity date.
- The CPB received updates on program level risks with a residual risk rating of 'extreme' or 'high' that included information on: residual and target risk severity; updates on control effectiveness and planned treatments; and changes in residual status.

2.25 Because PR3 was only assessed as 'high' between July 2025 and October 2025, it was only included in risk updates provided to the CPB at the August 2025 and November 2025[34] CPB meetings, despite being outside of the set risk tolerance level and overlapping with a 'high' rated strategic risk (SR5). This did not support effective monitoring of this key risk by the CPB. As discussed in paragraph 2.15, when the CEB and CPB did receive cyber security risk updates, the updates' usefulness was often limited by the accuracy and currency of the information submitted to the CPMO in response to risk update requests.

2.26 Both the CEB and CPB received information relevant to cyber security risks outside of formal risk updates. This was in the form of updates on the implementation of the Census Digital Service and myGov pathway for completing the Census, changes in the operating environment and use of social media for the 2026 Census program.

34 In November 2025, the CPB was advised that the residual risk rating had been reverted to 'medium' as the control effectiveness had returned to 'Substantially Effective'.

Cyber security risk deep dives

Risk deep dives conducted in September 2024 and December 2025 found that strategic cyber security risks were likely to be within the set risk tolerance level in time for the 2026 Census. A deep dive was also conducted on the Retrieval Augmented Generation chatbot, which was approved for use in the 2026 Census in December 2025.

2.27 The CEB conducted 'deep dives' into SR5 in September 2024 and December 2025. These involved analysis and reassessment of: risk severity; environmental and causal factors; control effectiveness; risk acceptability; potential consequences; and identification of new treatments, where applicable. Both deep dives concluded that while SR5 had a severity rating higher than the target severity rating at the time of the reviews, it would likely come within the set risk tolerance level ahead of the 2026 Census.

2.28 In May 2025, upon request of the CEB, the CPB undertook a deep dive into the risks and benefits of using a Retrieval Augmented Generation (RAG) chatbot for the ABS' 2026 Census website. In December 2025, the CEB confirmed 'Claire', a RAG chatbot, would be used as part of the Census Digital Services. The CEB was advised that the chatbot does not 'learn from its interactions and has the ability to be turned off quickly if adverse outcomes are detected.'

Oversight committees did not receive updates on critical cyber security controls in between strategic risk deep dives, including controls addressing potential sources of risk across the entirety of the ABS ICT environment.

2.29 Cyber security threats to the 2026 Census across all ABS ICT systems, not just systems implemented for the 2026 Census, were raised in the September 2024 strategic risk deep dive into SR5. The CEB was advised that:

> the threat landscape of this risk extends beyond Census to ABS IT systems. Although the scope of this Deep Dive focuses mainly on Census-managed controls, this report acknowledges the need to secure not only Census systems, but all others.

2.30 A suite of new risk treatments developed after the September 2024 deep dive were presented at the December 2025 deep dive. These had not been included in previous risk updates provided to the CEB between September 2024 and December 2025. The risk treatments included: hardening of the broader ABS ICT environment 'to ensure Census is not compromised by potential security vulnerabilities in supporting systems'; the formalisation of the Authority to Operate process; development of a Trusted Insider Threat Program[35]; and an 'Overarching Census security review and uplift'. The CEB was advised during the deep dive that these treatments were underway and 'will be enacted by Q2 2026.' As discussed in paragraphs 2.96 to 2.116, as at March 2026, sources of risk across the entirety of the ABS ICT environment remain a significant concern for the ABS and work is required to remediate the vulnerabilities.

35 The ABS developed its Trusted Insider Threat Program in response to Protective Security Policy Framework (PSPF) updates on 31 October 2024. PSPF Requirement 0051 is that: 'An insider threat program is implemented by entities that manage Baseline to Positive Vetting security clearance subjects, to manage the risk of insider threat in the entity'.
DHA, *PSPF Annual Release 2025*, p. 32.

Chief Security Officer (CSO) and Chief Information Security Officer (CISO) oversight

The ABS Chief Security Officer and Chief Information Security Officer are both involved in the monitoring of Census cyber security risks through involvement in Census governance committees.

2.31 The PSPF provides direction and guidance for 'Entity Chief Security Officers [CSO], Chief Information Security Officers [CISO], security advisers and other named security officials.'[36] It states that 'The CSO is responsible for the protective security practices and procedures, other than for cyber security, which are the responsibility of the CISO.'

2.32 In the ABS organisational structure, the ABS CISO reports directly to the CSO. For the 2026 Census, the CSO and CISO roles are embedded in the governance structure, as outlined in Table 2.3.[37]

Table 2.3 CSO and CISO committee involvement

Committee	CSO role	CISO role
CEB	Standing attendee	Attends by invitation
CPB	Member	–
Census Digital Services Project Governance Board	Deputy Chair	Member
ICT for Census Governance Forum	Chair	Member

Source: ANAO analysis of ABS documentation.

2.33 Under the 2026 Census governance structure, the Census Digital Services Project Governance Board and ICT for Census Governance Forum are technical subcommittees that report to the CPB. Both meet fortnightly and provide an opportunity to discuss and coordinate technical and project level cyber security matters.

- The CDS Project Governance Board is comprised of internal and external members and advisors. It operates as 'an advisory forum that brings together the critical stakeholders to discuss issues and decisions.' The CDS Project Governance Board is chaired by the ABS General Manager, Census & Population Division and the ABS CSO is the deputy chair.[38] Items discussed are specific to the CDS platform and relate to the Security Operations Centre, technical testing, development sprints, remediation of identified platform defects and management of open project level risks.

36 As a non-corporate Commonwealth entity, the ABS must apply the PSPF in accordance with Part 2 of the PGPA Act. Under the PSPF the:
- CSO is a Senior Executive Service (SES) officer responsible for oversight of the entity's protective security arrangements and provides strategic advice to the Accountable Authority.
- CISO supports the CSO by providing cyber security leadership, including responsibility for the entity's cyber security mitigation strategies.

DHA, *PSPF Annual Release 2025*, p. 5.

37 The CSO and CISO provide annual briefings to ABS senior leadership on enterprise-wide cyber security management, which includes an overview of Census cyber security.

38 In addition to the General Manager — Census & Population (chair) and CSO (deputy chair), members of the CDS Governance Board include: the Program Manager — Strategic Projects; the Program Manager — Security and Information Assurance; the Program Manager — Census 2026 (Collection) and an external member, a representative from Slalom. Internal advisors are the Director — Census Digital Service and Director TSD Census. External advisors are representatives from Slalom and AWS.

- ICT for Census Governance Forum is an internal forum chaired by the CSO. Items discussed in this forum relate to risks, security and ICT considerations for all Census systems. The forum is responsible for 'escalating issues … clarifying Program priorities' and 'managing delivery and security risk within the agreed risk appetite.'

2.34 A security audit conducted as part of the 2026 Census Security Work Program (see paragraphs 2.56 to 2.59) included a recommendation that ABS 'Increase the resourcing and or allocation of effort provided from SIA [Security and Information Assurance Branch] in providing external assurance of the Census Program'. The ABS agreed to the recommendation, stating that the 'Establishment of a Security Council to provide detailed overarching security governance, including formal Authority To Operate (ATO) processes' would be part of addressing the recommendation.

ABS Security Council

The ABS Security Council was created in June 2025 to address gaps in the monitoring of Census cyber security risks and assurance, and support the CSO and CISO in performing their roles. The Security Council's role as an advisory group in the 2026 Census governance structure was formalised in March 2026.

2.35 The Security Council's terms of reference state that it is 'an advisory group to the CSO and CISO to ensure timely decisions on significant security issues, risks and processes.' The ABS advised the ANAO in January 2026 that the Security Council commenced fortnightly meetings dedicated to 2026 Census security matters in June 2025. These meetings are attended by regular Security Council members[39], in addition to the Program Manager, Strategic Projects Branch and the Director, Census Security and Infrastructure. Representatives from Amazon Web Services (AWS) and Slalom attend the meetings as needed. Minutes were recorded from November 2025 and the Security Council's role as an advisory group within the 2026 Census governance structure was formalised in March 2026.

2.36 The Security Council has endorsed key decisions relating to the preparation for the 2026 Census, including: determining the appropriate thresholds for DDoS testing, security risks relating to the use of social media platforms for the Census and changes to the Security Operations Centre (SOC) following outcomes of the ORE.

2.37 The Security Council conducted a review of cyber security preparations following the August 2025 ORE and identified priorities for inclusion in a security uplift plan. In early November 2025, the Security Council briefed the SRO and other ABS senior executives[40] on the review and security uplift plan. The briefing noted that the CISO was leading the security uplift and would be 'working offline until December [2025] to focus on the Census Security Uplift'. As discussed in paragraphs 2.96 to 2.116, key remaining cyber security vulnerabilities must be addressed in time for the 2026 Census. This includes critical activities outlined in the security uplift

39 Security Council members include: the CSO (as chair); the CISO; the ITSA; the Security Assurance Lead (who simultaneously holds the role of Deputy ITSA), the Agency Security Advisor; the Chief Technology Officer; the Director of Cyber Operations; and the Australian Securities & Investments Commission's CISO (external member).

40 In addition to the SRO, the Deputy Australian Statistician — Chief Operating Officer, Chief Audit Executive and Chief Risk Officer and the General Manager, Census and Population attended the briefing.

plan. Establishing arrangements that support early identification and treatment of cyber security risks is essential for their effective management.

Recommendation no. 2

2.38 The Australian Bureau of Statistics establish cyber security advisory arrangements early in Census preparation to reduce gaps in risk monitoring and ensure effective mitigation across the breadth of ICT systems supporting the Census.

Australian Bureau of Statistics response: *Agreed.*

2.39 *The ABS is committed to ensuring risk monitoring and effective mitigation of cyber risks to the Census and the wider enterprise ICT systems on which the organisation relies. The ABS has focused on cyber security advisory arrangements throughout the design and development of the 2026 Census. The ABS Security Council formed in 2025 and was formally recognised in Census governance in early 2026.*

2.40 *The ABS Security Council serves as a core cyber security advisory and decision-making body to reduce gaps in risk monitoring and drive cyber risk management. The Security Council provides integrated cyber risk monitoring oversight and governance mechanisms for the purposes of Census Program and ABS foundational infrastructure. The Security Council will continue to govern security across the ABS beyond Census Main Event.*

2.41 *These changes address opportunities for improvement for the 2026 Census identified during the audit. This mechanism will ensure existing integrated security governance arrangements endure and support the 2031 Census Program.*

ABS Audit and Risk Committee

The ABS' Audit and Risk Committee received briefings on cyber security arrangements for the 2026 Census.

2.42 Under section 45 of the *Public Governance, Performance and Accountability Act 2013*, the accountable authority of a Commonwealth entity must ensure that an audit committee is established.[41] The ABS' Audit and Risk Committee (ARC) meets at least five times a year.

2.43 The ARC is required to review the appropriateness of the ABS' system of risk oversight and management.[42] It endorsed a program of activities, including briefings from the SRO and an external CEB member, to ensure it had visibility of the risk management and governance arrangements for the 2026 Census. Briefings to the ARC relating to 2026 Census cyber security arrangements included updates relating to: access to the 2026 Census through myGov; the outcomes of the December 2025 cyber security strategic level risk deep dive; the revision of the 2026 Census risk appetite statement; the Census program's security strategy, including the status of risk treatments;

41 Further requirements relating to audit committees are included under section 17 of the Public Governance, Performance and Accountability Rule 2014.

42 Department of Finance, *A guide for non-corporate Commonwealth entities on the role of audit committees 2021* Finance, Canberra, September 2021, available from https://www.finance.gov.au/publications/resource-management-guides/audit-committees-rmg-202 [accessed 4 March 2026].

engagement with cyber security experts; the use of AI for the 2026 Census (chatbot); and outcomes of the ORE, including incident management and business continuity processes.

Incident monitoring arrangements

The ABS is developing arrangements to detect and respond to cyber security incidents.

2.44 The Australian Signals Directorate (ASD) Information Security Manual (ISM) recommends organisations implement a cyber security continuous monitoring plan to support the accurate and consistent application of policies, processes and procedures for systems; and assist in proactively identifying, prioritising and responding to vulnerabilities. Control ISM-1163 is that:

> Systems have a continuous monitoring plan that includes:
>
> - conducting vulnerability scans for systems at least fortnightly
> - conducting vulnerability assessments and penetration tests for systems prior to deployment, including prior to deployment of significant changes, and at least annually thereafter
> - analysing identified vulnerabilities to determine their potential impact
> - implementing mitigations based on risk, effectiveness and cost.

2.45 In February 2025, the ABS endorsed a Census Digital Service (CDS) and Census Infosite Continuous Monitoring Plan[43], which 'establishes a consistent approach for the ongoing system monitoring and risk management for the Census Digital Services system'. This also supports the 'ongoing management and monitoring of security, risks and controls for the CDS and Census Infosite as defined by the ABS CDS System Security Plan.' The CDS and Census Infosite Continuous Monitoring Plan details: the ABS' vulnerability management plans and scanning arrangements; vulnerability assessment procedures; and security monitoring mechanisms in accordance with ISM-1163.

2.46 Under the CDS 2026 Event Incident Management Plan, the ABS will use a suite of monitoring tools during the 2026 Census that will be managed by ABS teams, third-party security firms, third-party cloud suppliers and Services Australia (the entity responsible for myGov).

2.47 Two Security Operations Centres (SOC) will operate during the 2026 Census.

- A third-party supplier will operate a SOC that monitors external systems on the CDS platform. During critical periods, the third-party SOC will be staffed continuously and systems will be actively monitored.
- The ABS will operate another SOC that monitors internal Census systems. AWS services include real-time monitoring of AWS applications and user experience monitoring. Cyber specialists will also assist the ABS during the Census Main Event when very high activity is expected to occur.

2.48 A system of alarms, notifications and escalations has been created based on threat analysis. When threshold values are reached, notifications are sent to on-call staff through predetermined

43 The CDS and Census Infosite Continuous Monitoring Plan was endorsed for use during the Operational Readiness Exercise and was being updated for Census 2026 at the time of review.

phone numbers, based on the priority level, which is determined through an incident priority matrix.

2.49 The CDS 2026 Event Incident Management Plan (EIMP) includes standard operating procedures (SOPs) with prioritisation guidance to be followed in the event of an alarm triggering. SOPs are mapped to alarm names (known as alarm messages) and include investigation steps that allow users to troubleshoot different scenarios.

2.50 Key objectives of the CDS monitoring systems include: receiving alarms based on pre-defined thresholds; indicating health status of the CDS workloads; trigger and guide event or incident response procedures; and verifying the effectiveness of incident responses. When a higher priority incident is triggered, the process requires that a triage call is activated and an Incident Response Team (IRT) convene in a dedicated 'Decide Room' to provide guidance and direction to the operational team.

2.51 Testing of incident monitoring arrangements has been conducted and is discussed in paragraphs 2.79 to 2.95.

Is the ABS conducting assurance and testing over cyber security controls?

2026 Census Assurance Plan and assurance schedule

2.52 In 2022, the ABS established the 2026 Census Program Assurance Plan (the plan), which defines the scope and timing of assurance activities to provide transparency and confidence that the program is on track and managing risks appropriately. The CEB provides oversight for the implementation of the plan and receives reporting on the findings of some assurance activities.[44] The CEB is required to be consulted on amendments to the plan. The ARC reviewed the plan in May and December 2023. Updates to the ARC included information on outcomes of assurance activities outlined in the plan.

2.53 The plan was updated in 2024 and twice in 2025, following requests from the Digital Transformation Agency (DTA), and the DTA reviewed it as required for Tier 2 programs.[45] Changes made in response to DTA reviews included adding how lessons learnt from previous Censuses had been incorporated into the assurance approach and clarifying roles and responsibilities.

44 The CEB received reporting on third line assurance activities but not second or first line assurance activities (see Footnote 46 for a description of the lines of assurance and Table 2.4 for a list of second and third line assurance activities for the 2026 Census).

45 As discussed in paragraph 1.18, the DTA provides oversight of delivery of digital and ICT initiatives under the Digital and ICT Investment Oversight Framework. Separate to its internal assurance program, the ABS met DTA requirements to provide biannual 'assurance activities that provided a Delivery Confidence Assessment rating on the overall health of the investment' in the form of wave reports.

2.54 The assurance model for the 2026 Census is based on the 'three lines of assurance' model.[46] The plan states it 'has been designed to target assurance to known risk areas based on the 2021 Census cycle and key emerging issues'. The plan includes an assurance schedule that provides high level information on the timeframes and scope of each type of activity, as well as who would be responsible for undertaking the activities.

2.55 The ANAO has reviewed both the second line and third line assurance activities that were directly related to cyber security, as outlined in Table 2.4. In addition, the Australian Cyber Security Centre (ACSC), which is 'the Australian Government's technical authority on cyber security,' has been providing assistance to the ABS as part of its preparations for the 2026 Census Main Event.

Table 2.4 2026 Census Program Assurance Plan second line and third line assurance activities

Activity	Second line assurance	Third line assurance
Cyber security related	• 2026 Census Security Work Program • Quality Gates	• Gateway-style Review Program • Program Advisor • Specialist Review Program • Reviews by cyber security specialists
Other assurance activities	• 2026 Census Program Strategy • 2026 Census Privacy Impact Assessments • 2026 Privacy Strategy Suite (2026 Census PIA Plan, 2026 Census Data Protection Plan, 2026 Census Privacy Plan)	• Internal Audit Program • Statistical Independence Assurance Panel • Privacy Advisor

Source: ABS documentation.

2026 Census Security Work Program

The ABS established an appropriate program of security testing and assurance activities for the systems that will be utilised in the 2026 Census. Assurance activities and testing are being conducted in line with planned timeframes of the Security Work Program. Gaps were identified in architecture and design reviews.

2.56 In November 2022, the ABS established a program of security testing and assurance activities under the 2026 Census Security Work Program. The program outlines a schedule of testing for the systems that will be utilised in the 2026 Census. Testing requirements were determined

46 A similar approach was used for the 2021 Census. The description of the model contained in the 2026 Census Program Assurance Plan is:

> **The first line** is formed by managers and staff who own and manage risks at the project and program levels. They mitigate and resolve risks and escalate issues as appropriate. …
>
> **The second line** is formed by organisational functions or cross cutting program roles that oversee or specialise in compliance or the management of risk. This includes IT Security, Program Management Office, Finance, Census quality, Testing and Privacy teams. …
>
> **The third line** is provided through independent and objective assurance and advice on all matters related to achieving the Program objectives. Independent assurance can be initiated by the Program or by the external bodies with the authority to audit the Program.

based on system risk profiles set out in the 2026 Census Security Strategy. Systems were given a priority number from one (highest priority) to eight (lowest priority), based on factors including whether the systems were public facing and whether they contained personally identifiable information and/or unit record data.

2.57 The ABS advised the ANAO in January 2026 that in addition to system risk profiles, the frequency and scope of testing in the 2026 Census Security Work Program was also informed by other factors. These included insights from the 2021 Security Strategy and Program Delivery, Census and other system release timelines, personnel resourcing, budget considerations, and findings from security assurance activities.

2.58 The Census Security Work Program comprises cyber security risk management activities, as outlined in the 2026 Census Security Strategy, with a summary provided below.

- **Distributed denial of service (DDoS) testing**: simulates a cyber attack designed to load a network with so much malicious traffic that it cannot operate or communicate as it normally would. DDoS testing was conducted over the Census Digital Service (CDS) prior to the Operational Readiness Exercise (ORE), with further DDoS testing of the CDS and other high risk public facing systems scheduled during 2026.
- **Penetration testing** (also known as 'ethical hacking'): a security exercise where cyber security experts attempt to find vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a system's defences that attackers could exploit.
- **Information Security Registered Assessors Program (IRAP) assessments**: an Australian Signals Directorate (ASD) initiative to provide information technology security assessment services to government. The ASD endorses information technology professionals to provide security services with the aim to secure broader industry and Australian Government information systems.
- **Biannual security audits**: cloud security and architecture reviews conducted by third-party suppliers.
- **Code reviews**: reviews of code changes prior to deployment to identify bugs, potential security vulnerabilities, and ensure consistency with overall system architecture.
- **Security risk assessments**: articulation of the security risk posture of an ICT solution and identification of corresponding security risks and risk treatments. This is documented in Security Risk Management Plans and System Security Plans and reviewed in IRAP assessments.
- **Architecture and design reviews**: architecture diagrams showing how systems are structured are developed for all new ICT systems and systems undergoing significant review and endorsement before security teams assess appropriateness of the design and the system progresses from development to production. Security architecture and design processes are detailed in security risk assessment documentation.
- **Protective security site reviews**: assessments conducted over facilities hosting sensitive Census information including data centre facilities and infrastructure hosting Census systems and information.

2.59 Cyber security risk management activities are being conducted in line with the planned timeframes of the Security Work Program; gaps were identified in architecture and design reviews.

Architecture and design reviews

2.60 Auditor-General Report No.16 2020–21 *Planning for the 2021 Census* identified that Census systems did not fully align with the ABS enterprise ICT framework, giving rise to risks in relation to system integration and compliance with legislation and ABS policy. The report included a recommendation that the ABS strengthen its IT framework and assess how non-compliance with standard architectures could impact its compliance with legislative and policy requirements.[47]

2.61 All 2026 Census ICT systems must undergo an architecture and design review under the 2026 Census Security Strategy. A cyber security review conducted in August 2025 identified gaps in high-level architecture documentation across parts of the Census program. The review found that some systems presented for security assessment contained limited architectural detail, relying on security context documents rather than full architecture documentation, which limited the ability to assess security design.

2.62 Where high-level architecture documentation was inadequate to conduct a security architecture review, ABS security assessors combined security risk assessment documentation with architecture and design documentation to analyse specific controls from a security perspective. The ISM specifies that systems' cyber security architecture documentation should be approved by the system's authorising officer prior to the development of the system (Control: ISM-1739) and reviewed annually (Control: ISM-0888).

Recommendation no. 3

2.63 The Australian Bureau of Statistics comply with the Information Security Manual requirements by:

(a) ensuring comprehensive architecture documentation is prepared and approved prior to developing ICT systems; and

(b) reviewing security architecture documentation annually.

Australian Bureau of Statistics response: *Agreed.*

2.64 *The ABS is committed to satisfying its obligations to adhere to Information Security Manual control requirements including those specific to the preparation and approval of comprehensive architecture documentation before ICT system development and annual review of security architecture documentation.*

2.65 *The ABS has produced comprehensive architecture documentation for 2026 Census systems, and these are captured within Security Risk Management Plans (SRMPs) which serve as key artefacts in the formation of Census system Authorities to Operate.*

47 ABS documentation indicates that the recommendation was implemented in April 2021.

2.66 *The ABS has reviewed Authorities to Operate templates and built 12-month review gates into its cyber Governance, Risk and Compliance tool to ensure security architecture documentation is reviewed on an annual basis with technical owners as part of system reaccreditation processes.*

2.67 *These changes address opportunities for improvement for the 2026 Census identified during the audit.*

Engagement with cyber security experts

2.68 The ABS is receiving advisory services and technical support from cyber security experts as they prepare for the 2026 Census. Specialist teams are carrying out protective and detective cyber security scanning, monitoring and vulnerability testing across the ABS' ICT environment and primary ICT platforms. The ABS is also receiving expert advice on matters of cyber security and emerging threats. As discussed in paragraph 1.15, the ACSC is providing support and assistance to the ABS.

Quality gates and gateway-style reviews

Quality gates and gateway-style reviews are designed to provide assurance of quality and compliance. There are gaps in how the quality gates are being monitored and reported.

2.69 The 2026 Census Program Assurance Plan includes 'quality gates' and 'Gateway-style' program reviews. These activities differ from the Gateway Reviews facilitated by the Department of Finance (Finance) for major Australian Government projects and programs.[48] Quality gates are conducted by ABS staff (second line assurance activity), while the gateway-style reviews are conducted as a third line assurance activity by a review team comprised of three reviewers.[49]

Quality gates

2.70 A 'quality gate' is a 'set of acceptance criteria to test the overall quality of process outcomes at pre-determined points.' The quality gate process provides assurance that:

- each Census ICT system has been thoroughly tested[50];
- associated security activities have been conducted[51]; and
- all business processes are complete.

2.71 Quality gates also provide assurance that cyber security measures align with organisational standards and compliance requirements. Evaluation of the 2021 Census process recommended reusing the same quality gate approach for the 2026 Census, concluding that the gates were

48 Finance may recommend a Gateway Review process be conducted for projects and programs above a certain threshold.
Department of Finance, *Gateway Reviews Process*, Finance, Canberra, 19 December 2025, available from: https://www.finance.gov.au/government/assurance-reviews-and-risk-assessment/gateway-reviews-process [accessed 16 January 2026].
The ABS advised the ANAO in January 2026 that 2026 Census preparations were not subject to the Department of Finance-led Gateway Reviews.

49 The ABS advised that a targeted approach to select independent panel members was adopted, with limited tender procurements undertaken for each of the panel members.

50 System testing is documented in an Assurance Minute.

51 Security elements are documented in an Authority to Operate approval. Prior to 2025, security elements were documented in an Assurance Minute.

'extremely valuable in providing the Senior Responsible Officer and Census Executive with assurance that key activities and processes were ready to go live for operations.'

2.72 The 2026 Census quality gate schedule has three key phases:

- 2024 Census Test (which did not proceed — see paragraph 1.9);
- 2025 Operational Readiness Exercise; and
- Main Event 2026 Census.

2.73 As at March 2026, quality gates containing a security measure have been conducted in accordance with the timeframes established in the 2026 Census Program Assurance schedule. Review workshops were scheduled for April 2024, November 2024, February 2025 and November 2025 to determine the relevance of upcoming gates, identify potential new gates and analyse the effectiveness of those completed. These workshops were not held and the rationale was not documented. The ABS advised the ANAO in January 2026 that it chose to adopt an 'agile approach to planning the Quality Gate timetable, delivering education and determining which gates were required'.

2.74 The ABS advised the ANAO in December 2025 that 30 completed quality gates contained a security measure whereby 'security documentation is reviewed and endorsed by ABS IT Security'.

- Twenty-six were cleared, meaning that all quality measures were satisfied.[52]
- The four that were conditionally cleared had outstanding residual risks relating to completion of technical configuration, data management and review of security documentation for specific systems and processes.
  - Post gate activities (PGAs), which 'can't be done at the time the gate is signed off but are an important part of the gate's quality assurance' were completed for the four quality gates. Of these, one gate was missing the required sign off to confirm a PGA had been completed, three gates were missing evidence supporting the activity's completion, and three gates had activities that were completed after the due date.
- Inaccurate and incomplete documentation indicates there may be gaps in how the quality gates are being monitored and reported.

Gateway-style reviews

2.75 Annual gateway-style reviews have been conducted since 2023 to provide assurance to the SRO at critical points of the 2026 Census program. Each review included three reviewers. Reviewers were procured by the ABS through a limited tender approach to ensure reviewers had the 'appropriate diversity and depth of specialist skills and experience to provide valuable and trusted advice on the Program'. As at March 2026, all three completed reviews produced a 'delivery confidence assessment' of 'green/amber' on the overall success of the 2026 Census and recommendations for improvement. This indicated that 'successful delivery appears probable however constant attention will be needed to ensure risks do not materialise into major issues

52 There are three gate outcomes: cleared, conditionally cleared and failed.

threatening delivery'.[53] Cyber security was addressed under the 'Technology and Security' heading of each review.

- 2023: the review concluded that 'the ABS [had] woven cyber into the fabric of the Program from the start, not as an afterthought.'
- 2024: the review found that 'Suitable security-related testing has been flagged so the Review team is confident that the Program is well prepared to manage this risk.'
- 2025: the review concluded that 'Cyber security is a prominent risk, and the Program Team is undertaking appropriate measures, including the use of third parties to ensure that appropriate protection is in place'. The review recommended that the ABS 'Ensure the ongoing development of detailed incident and crisis response plans to address potential disruptions to the Census and prioritise refinement of business continuity strategies to enable swift and effective response to crises.'

2.76 The final gateway-style review is scheduled for May 2026 and will focus on data operations.

Program Advisor

2.77 The Program Advisor provides advice to the SRO and Australian Statistician following CEB meetings. The Advisor's role includes '[to] review and challenge the effectiveness of preparations for the 2026 Census'. For the 2026 Census, the ABS contracted the former Deputy Australian Statistician and SRO through a limited tender procurement process. The ABS advised the ANAO in December 2025 that cyber security was discussed on one occasion in December 2025, where the Advisor supported additional treatments being put in place following the cyber security strategic level risk deep dive (see paragraph 2.27).

Specialist Review Program

2.78 The Specialist Review Program involves a series of reviews by external subject matter experts to provide assurance over the design, planning or readiness of elements of the 2026 Census. Topics are selected by the CEB. In line with the assurance schedule, the ABS has completed a minimum of two reviews each year from 2023 to 2025. The ABS advised the ANAO in March 2026 that review topics had not yet been selected for 2026. As at March 2026, one specialist review had been conducted by EY that included coverage of cyber security risks.[54] The review assessed data processing and coding systems and made three recommendations to address observations related to cyber security and controls. None were at the program level, and all were given a priority rating of 'medium' or below.[55] ABS documentation from February 2026 indicated that all three recommendations had been implemented.

53 The delivery confidence assessment uses the colours 'green' ('successful delivery appears highly likely'), 'amber' ('successful delivery appears feasible but significant issues already exist requiring management attention') and 'red' ('successful delivery appears to be unachievable') to indicate status. Results that are on the border of the assessment categories include both colours (for example, 'green/amber' or 'amber/red').

54 The ABS approached a single supplier (EY) through the Digital Marketplace panel.

55 Medium priority recommendations indicate that 'some clarity and/or changes needed; potential risk to successful delivery; actions recommended'.

Cyber security detection and incident management testing

Testing for detection and incident management has been conducted based on potential attack vectors identified through threat modelling. Testing confirmed that the monitoring systems are active and identifying issues as they arise, and appropriate procedures were followed through to conclusion of events.

2.79 The PSPF defines security incident management as 'the process of identifying, managing, recording and analysing any irregular or adverse activities or events, threats and behaviours in a timely manner.'[56] PSPF Requirement 0026 is that 'Procedures are developed, implemented and maintained to ensure security incidents are responded to and managed.'

2.80 Following the events of the 2016 Census, a review was conducted by the Special Adviser to the Prime Minister on Cyber Security (known as the MacGibbon Review). A key finding of the MacGibbon Review was that 'the ABS had no clearly identified and tested cyber security incident response processes.' This resulted in 'ad hoc decision making' during the 2016 Census cyber security incident. The review noted that:

> the ABS … had a library of at least six incident management documents to guide them through Census night … None of the documents outlined a comprehensive cyber incident response plan to be followed on Census night … The documents suffered from inconsistent definitions, unclear processes, a lack of focus on cyber incidents and an absence of thorough testing.[57]

2.81 ABS documentation states that the 2026 Census would include arrangements implemented for the 2021 Census that addressed findings of the MacGibbon Review, including:

- scenario planning where incident and/or crisis management might be required;
- preparing for emerging incidents and emergencies by assessing, triaging, escalating and actioning accordingly;
- undertaking incident management training across the Census program; and
- development of action plans for possible incidents and/or emergencies that might occur.

2.82 These actions have been addressed through the ABS' 2026 Census cyber security incident management arrangements. Threat modelling was conducted and used in scenario planning for incident response simulations (see paragraph 2.86), preparation for incidents and emergencies is documented in the CDS Incident Management Plan (see paragraph 2.83), incident management training is being conducted (see paragraph 2.93) and incident and emergency action plans are documented in the 2026 Census Issues and Crisis Management Action Plan (see paragraph 2.83).

---

56 The PSPF defines a security incident as an:

- action, whether deliberate, reckless, negligent or accidental, that fails to meet protective security requirements or entity-specific protective security practices and procedures that results in, or may result in, the loss, damage, corruption or disclosure of official information or resources
- attempt to gain unauthorised access to official information or resources
- approach from anybody seeking unauthorised access to official resources, or
- event that harms, or may harm the security of Australian Government people, information or resources.

DHA, PSPF Annual Release 2025, p. 12.

57 MacGibbon, *Review of the Events Surrounding the 2016 eCensus*, pp. 20–21.

2026 Census cyber security incident management arrangements

2.83 The ABS maintains a suite of documents underpinning its incident response procedures for the 2026 Census, in accordance with PSPF Requirement 0026. These are:

- **Census Issues and Crisis Management Framework:** aligned to the Australasian Inter-Service Incident Management System (AIIMS) and the Australian Government Crisis Management Framework (AGCMF).
- **2026 Census Issues and Crisis Management Strategy**: defines the direction, objectives and scope of issues and crisis management for the 2026 Census Program.[58]
- **2026 Census Issues and Crisis Management Action Plan**: triggered when a cyber or security incident related to the Census is identified.[59] Describes actions to be taken and timeframes for completion, and includes links to incident management plans and templates.
- **Census Digital Services 2026 Event Incident Management Plan**: describes event and incident management processes; monitoring arrangements; and escalation paths, incident management workflow and checkpoints. It also details the roles and responsibilities of operational teams in monitoring applications; remediating technical and security issues; driving business decisions; managing Census-wide issues; and providing technical guidance.

2.84 The ABS has an Issues and Crisis Communication Plan and has an established process for managing media and public communications during issues and crises. The ABS has drafted pre-approved public communications releases that will be shared across Census channels in the event of an issue or crisis.

Testing of 2026 Census incident response arrangements

2.85 The PSPF recommends that organisations undertake regular exercises of security incident management arrangements.

> A security exercise tests the entity's preparedness to detect, respond to and recover from all types of security incidents. It also tests whether the entity's security incident management plans are appropriate and effective.[60]

2.86 In July 2024, a third-party supplier conducted a threat modelling assessment against the Census Digital Service (CDS). The assessment identified potential attack vectors that were 'used to aid the development of detection logic to monitor for security threat events' and develop scenarios for incident response simulations. CDS incident management simulations and testing have taken place in two phases.

- Phase 1 simulations occurred during May and June 2025, which consisted of presentations, workshops and scenario-based role play exercises.

58 The 2026 Census Issues and Crisis Management Strategy was endorsed for use during the Operational Readiness Exercise and was being updated for the 2026 Census at the time of review.

59 The preparation of issues and crisis action plans is a quality measure to the relevant quality gates, which are required to be passed prior to a service 'going live'.

60 DHA, *PSPF Annual Release 2025*, p. 13.

- Phase 2 planned systems testing and simulation took place during the CDS Operational Readiness Exercise in August 2025.

2.87 Phase 2 testing was conducted during the ORE, with the ABS SOC and third-party SOC providing additional on-call support. This testing included a 'complex series of overlapping security events' to test incident response and system capability over a three-day period. Malicious activity included attack vectors identified in the threat modelling assessment.

2.88 Alerts were triggered and the defined process was followed to commence the incident management process, with triage calls conducted and the 'Decide Room' convened. At the conclusion of the exercise, the ABS reported that:

> attack vectors … were successfully mitigated by a variety of defence mechanisms that were enacted by the internal teams with support from AWS. All CDS platform services remained stable during and after the incident with no end-user or system impacts.

2.89 The report concluded that cross team collaboration enabled highly effective and well-rehearsed incident and event management processes, helping teams diagnose and mitigate threats; and that continuous monitoring by several teams minimised the likelihood of any issues going undetected.

2.90 This simulated security incident identified the following areas for improvement:

- improved alignment between monitoring and alerting mechanisms in the ABS and with third-party suppliers;
- improved visibility of the support schedule for 'eyes on glass'[61] monitoring compared to alarm-based alerts; and
- detailed simulations across stakeholders to strengthen the incident and event management process.

2.91 The ABS made changes to alerting systems as a result of this simulation.

2.92 The ABS deemed Phase 2 systems testing and simulation 'excellent preparation for the forthcoming [Census] Main Event' that 'enabled project teams to refine their processes and systems … which increased confidence in managing issues and crises.' The ABS also asserted that the ORE demonstrated how the Census Program matured its understanding of issues and crisis management, including preparedness activities that enable timely and structured responses to challenges.

2.93 Further operational and security testing of the CDS, incident response arrangements and monitoring systems is scheduled to take place over the months prior to the 2026 Census. Further CDS incident management simulation activities are also scheduled to occur ahead of the 2026 Census. The planned activities include:

- scenario-based role play;
- communication processes and paths;
- triage meetings;
- technical analysis; and

61 'Eyes on glass' is a cyber security term for continuous, human monitoring of a system through a dashboard or console to detect and respond to threats.

- incident resolution.

2.94 The ABS' 'approach to cyber security detection and incident management testing is one of continued testing, analysis and improvement.' The ABS has assured itself that this is the right program of detection and testing through 'expert advice from a range of premier Government security agencies, Industry experts, platform partners and … experience in conducting successful Census cycles.'

2.95 The ASD's 2024–25 Cyber Threat Report stated that there had been increases in various forms of cyber incidents across business and government. The PSPF and ISM provide requirements and guidance for entities in the management of cyber incidents, and testing of response arrangements can provide assurance that risks associated with an incident are being effectively managed. The ABS has taken a risk-informed approach to testing incidents based on identified threats to the 2026 Census.

Are there plans in place to address identified issues in cyber security controls in time for the 2026 Census?

Cyber security uplift plan

The ABS established a security uplift plan in November 2025, and actions are being monitored by the ABS Security Council. As at March 2026, plans have been established to address identified issues. The ABS has assigned 'amber' ratings to certain actions, and efforts to uplift the broader ABS ICT environment are self-assessed as a 'medium-high' risk.

2.96 As discussed in paragraph 2.37, the ABS established a security uplift plan following a Security Council cyber security review after the August 2025 ORE. The plan outlined the following actions but did not specify timeframes or assign responsibilities:

- reassess security assurance activities to ensure assessments are comprehensive, appropriately track and prioritise residual risk treatments, and cover all Census systems and supporting business as usual systems;
- improve data security through system controls and data governance;
- uplift the broader ABS ICT environment;
- establish the Trusted Insider Threat Program with specific reference to Census risks;
- improve plans, processes and playbooks for cyber incident responses;
- collaborate with experts and vendors to uncover blind spots; and
- increase visibility of the Security Work Program and residual risks through reporting.

2.97 At the December 2025 cyber security risk deep dive (see paragraph 2.27), the proposed treatments presented to the CEB were:

- risk assessment, vulnerability management and hardening of the broader ABS ICT environment;
- a more formal approval process for new and changed ICT systems ('Authority to Operate');
- enhanced personnel security measures through the Trusted Insider Threat program; and
- an 'overarching Census security review and uplift'.

2.98 From 18 November 2025, the Security Council received consistent reporting on the progress towards actions outlined in the security uplift plan. The status of all actions has remained 'amber'[62] or below for the period between December 2025 and March 2026, except for a 'red' rated action to 'uplift the wider ABS security environment'.[63]

Security across the broader ABS ICT environment

The ABS gave insufficient consideration to holistic cyber security planning for the 2026 Census as it did not address risks across the entirety of the ABS ICT environment. Similar issues were observed in Auditor-General Report No. 16 2020–21.

PSPF security mitigation strategies

2.99 In 2023 and 2024, the ABS conducted PSPF self-assessments[64] in which it assessed that cyber security components had not yet achieved target levels.[65] Following the 2024 assessment the ABS implemented a security uplift project to improve cyber security maturity with a target date of June 2025. In the September 2025 PSPF self-assessment, additional security controls had been implemented to reduce risks, but cyber security compliance remained below target levels. The ABS had developed, implemented and maintained a cyber security strategy and uplift plan, however, did not implement all key mitigation controls.

2.100 As of March 2026, the CEB received updates indicating that efforts were underway to address the identified challenges in implementing the Essential Eight mitigation strategies.

Census cyber security risks across the ABS' broader ICT environment

2.101 Auditor-General Report No.16 2020–21 *Planning for the 2021 Census* concluded that the ABS established partly appropriate cyber security measures for the 2021 Census. This report identified a risk that cyber security strategies would not be implemented in time to provide sufficient coverage over the broader ABS ICT environment for the 2021 Census. The report included a recommendation aimed at strengthening cyber security by defining timeframes and responsibilities for implementing the 2021 Census Security Strategy and the ABS' Essential Eight Uplift Program.[66]

2.102 The September 2024 CEB strategic risk deep dive (see paragraph 2.27) identified that there were cyber security threats to the 2026 Census stemming from all ABS ICT systems, not just systems

62 The ABS advised the ANAO that the definitions of colour-coded status are incorporated in a project management program proforma. The amber rating is defined as: 'Specific components of the project are facing significant issues (design, schedule, resourcing, etc) which might put the project off track if they persist. Proposed actions … need careful management attention until the cause is no longer a threat ('watch')'.

63 The red rating is defined as: 'Specific components of the project and/or the project overall is 'at risk'. Remedial actions are required to bring the project back on track and need careful monitoring in the governance process ('remediate')'.

64 Australian non-corporate Commonwealth entities (NCEs) must complete an annual self-assessment as a measure of their security maturity against the PSPF. Entities are required to implement the mitigation strategies to at least Maturity Level 2, the level in which the majority of PSPF core and supporting requirements have been implemented. An entity's implementation of the Essential Eight mitigation strategies is the core component of 'cyber security hardening', or reduction in the likelihood of an ICT system being compromised.

65 The ABS' self-assessment included all ABS systems, including Census systems.

66 ABS documentation indicates that the recommendation was implemented in April 2021.

implemented for the 2026 Census. The need to secure all systems across the ABS' ICT environment was identified.

2.103 Following the August 2025 ORE, the Security Council's cyber security review found that dependencies and risks associated with the broader ABS ICT environment were not clearly tracked or reflected in the Census security posture. It recommended that the business-as-usual cyber security work program be reviewed and better integrated with Census cyber security risk management.

2.104 In the December 2025 strategic risk deep dive, the CEB was again advised of the need to secure all systems across the broader ABS ICT environment, and to anticipate the occurrence of increased cyber activity in the lead-up to the Main Event in early 2026. The suite of controls that include 'Risk assessment, vulnerability management and hardening of the broader ABS IT environment' was reported as 'substantially effective' and 'on track for Main Event.'

2.105 From 15 January 2026, the ABS Security Council incorporated consideration of risks and dependencies associated with Census systems and the broader ABS ICT environment in its assessment of 2026 Census cyber security risks. The reported status of the overall 'security program in preparation for Census' was rated as 'red'[67] with an aggregated security risk of 'medium-high'.

2.106 The risk was considered at subsequent Security Council meetings, including a briefing to the SRO and COO on 9 February 2026, where additional funding was sought. At the 25 January 2026 Security Council meeting, the 'forecast residual risk' was lowered to 'medium' from 'medium-high', bringing it to within the revised risk tolerance level established in December 2025, when it was changed from 'low' to 'medium' (see Table 2.2). The justification for the lower risk ratings was not evident as all risk factors that previously warranted a higher rating remained relevant. Between 15 and 27 January 2026, reference to a risk of insufficient budget for procuring resources to conduct security assessments was removed from reporting, however that risk remained unresolved during this period.

2.107 At the 9 February 2026 briefing, the SRO and COO requested further clarification around funding pressures and current mitigations against environment cyber risks. It was noted that:

> Scheduled completion of the foundation infrastructure and enterprise system security assessments is very close to ME [Main Event] and there is no contingency in the schedule … Funding for contractors delivering [these assessments] … currently expires in March [2026].

Once the scale of cyber security vulnerabilities affecting preparedness for the 2026 Census became apparent, the ABS quickly identified the need for additional cyber security expertise, which has since been engaged.

2.108 The ABS advised the ANAO in January 2026 that it anticipated hardening of the ABS ICT environment would be executed in three consecutive, two-month tranches of work. In February 2026, the ABS stated that to mitigate the risk it had 'defined a prioritised program of security hardening activities, which are being progressed' and that:

> cyber security uplift is ongoing, and while residual risks cannot be fully eliminated before the 2026 Census, they are being actively managed … Multi-layered assurance and the ABS' continuous

67 See Footnote 63 for the description of the red rating.

reassessment provides strong confidence that any significant issues will be identified and addressed ahead of Census.

2.109 In January 2026, the ABS engaged specialists to 'uplift and harden' the ICT and cyber security environment ahead of 2026 Census Main Event. The team was originally planned to work with the ABS for a four-week period; this was extended to last for between three to six months. In addition, the ABS engaged significant additional cyber security support from mid-February 2026.

To be ready for the 2026 Census, the ABS must ensure critical activities will be completed in time.

2.110 In March 2026, the Security Council continued to rate the foundation infrastructure and enterprise system security risk as 'medium-high', with concerns remaining regarding the need to complete security assessments amid funding and resourcing uncertainty. The ABS was operating under constrained budget and resourcing conditions, scheduling of IRAP assessments was incomplete, and gaps in information and documentation were delaying some assurance activities. IRAP assessments that should have been completed had not yet commenced and tender responses from IRAP assessors indicated that 'due to the scope … assessments will take up to 3 months to complete, which does not align with the schedule.' If IRAP assessments are able to be completed, there may be insufficient time to implement the resulting findings and recommendations before the 2026 Census.

2.111 The systems hardening program encompasses a large scope of work across the broader ABS ICT environment. The ABS has been working to address identified challenges in cyber security components of the Essential Eight mitigation strategies since 2023 but has repeatedly missed deadlines for achievement. The ABS has allocated additional resources to deliver systems hardening in time for the 2026 Census and is proceeding according to a prioritised schedule of activities. As at March 2026, the 'residual risk level' remains self-assessed at 'medium-high'. As was found in Auditor-General Report No.16 2020–21 regarding preparation for the 2021 Census, to be ready for the 2026 Census the ABS must address key remaining cyber security vulnerabilities by ensuring critical activities will be completed in time.

Recommendation no. 4

2.112 The Australian Bureau of Statistics ensure that:

(a) the assessment and mitigation of risks to cyber security readiness stemming from the broader ABS ICT environment, including critical systems hardening requirements, are incorporated into Census ICT frameworks; and

(b) risks identified in audits and review activities are adequately addressed in planning and strategy documents.

Australian Bureau of Statistics response: *Agreed.*

2.113 *The ABS is confident that its multi-layered assurance and continuous reassessment of the threat environment mean significant cyber issues will be identified and addressed ahead of the 2026 Census.*

2.114 *The ABS recognises the vital role that the Census ICT framework plays in assessing cyber security readiness for the Census Program, and that broader ABS ICT environment risk posture and critical system hardening are central tenants in formulating this integrated readiness*

assessment. An end-to-end security approach has been applied to all 2026 Census release cyber documentation, and assessments consider control and risk inheritance from underlying foundational infrastructure.

2.115 *The ABS is currently refreshing the Cyber Security Strategy and material findings from audit and review activities will be incorporated into the new strategy. Cyber security planning is embedded within enterprise risk management, executive governance, and event readiness processes, with regular reporting to the Executive Board, Census Executive Board, and the Audit and Risk Committee. The ABS continuously reassesses threats and risks, prioritises controls for critical systems, adjusts sequencing and investment as vulnerabilities emerge, and integrates planning across Census and non-Census ICT systems.*

2.116 *This work addresses opportunities for improvement for the 2026 Census identified during the audit. The ABS will continue to build on work underway.*

Dr Caralee McLiesh PSM
Auditor-General

Canberra ACT
18 May 2026

Appendices

Appendix 1 Entity response

Australian Bureau of Statistics
Locked Bag 10 | Belconnen ACT 2616

Ref: EC26-000099

Dr Caralee McLiesh PSM
Auditor-General
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Caralee

The ABS appreciates the opportunity to respond to the ANAO proposed report on the *Cyber Security Readiness for the 2026 Census* under section 19 of the *Auditor-General Act 1997*.

The ABS acknowledges the findings of the report and agrees to the four recommendations, noting that all will be implemented before the 2026 Census. This audit has complemented an extensive assurance and testing program that has supported the 2026 Census. The recommendations are consistent with the ABS's commitment to best practice governance, risk management and continuous improvement.

The ABS continuously reassesses cyber threats and risks, prioritises controls for critical systems, actively adjusts sequencing and investment as vulnerabilities emerge, and integrates planning across Census and non-Census IT systems. The ABS is confident that its multi-layered assurance and continuous reassessment of the threat environment mean we will be ready to deliver the 2026 Census.

The ABS' summary response to the proposed audit report and response to each recommendation is provided at **Attachment A,** and editorial matters the ABS wishes to bring to the ANAO's attention are provided at **Attachment B.** If you would like further information regarding this response, please contact Siobhan Campbell, Program Manager, Enterprise Management Branch, on 02 9268 4235 or siobhan.campbell@abs.gov.au.

Lastly, I take this opportunity to thank the ANAO for its professional and productive engagement throughout the audit.

Yours sincerely,

David Gruen

Dr David Gruen AO
Australian Statistician
13 May 2026

www.abs.gov.au