

The Auditor-General
Auditor-General Report No.1 2019–20
Performance Audit

Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities

Australian Postal Corporation

ASC Pty Ltd

Reserve Bank of Australia

© Commonwealth of Australia 2019

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 978-1-76033-478-9 (Print)

ISBN 978-1-76033-479-6 (Online)

Except for the content in this document supplied by third parties, the Australian National Audit Office logo, the Commonwealth Coat of Arms, and any material protected by a trade mark, this document is licensed by the Australian National Audit Office for use under the terms of a Creative Commons Attribution-NonCommercial-NoDerivatives 3.0 Australia licence. To view a copy of this licence, visit <http://creativecommons.org/licenses/by-nc-nd/3.0/au/>.

You are free to copy and communicate the document in its current form for non-commercial purposes, as long as you attribute the document to the Australian National Audit Office and abide by the other licence terms. You may not alter or adapt the work in any way.

Permission to use material for which the copyright is owned by a third party must be sought from the relevant copyright owner. As far as practicable, such material will be clearly labelled.

For terms of use of the Commonwealth Coat of Arms, visit the *It's an Honour* website at <https://www.pmc.gov.au/government/its-honour>.

Requests and inquiries concerning reproduction and rights should be addressed to:

Senior Executive Director
Corporate Management Group
Australian National Audit Office
19 National Circuit
BARTON ACT 2600

Or via email:

communication@anao.gov.au.





Canberra ACT
4 July 2019

Dear Mr 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 Postal Corporation, ASC Pty Ltd and the Reserve Bank of Australia. The report is titled *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*. 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

A handwritten signature in black ink that reads 'Grant Hehir'.

Grant Hehir
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 his 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
Fax: (02) 6203 7777
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

Esther Barnes
Edwin Apoderado
Kelvin Le
Jason Ralston
Carissa Chen
David Ma
David Willis
Bola Oyetunji
Andrew Morris

Contents

Summary and recommendation	7
Background.....	7
Conclusion	8
Supporting findings.....	8
Recommendation	10
Summary of entity responses	10
Key messages from this audit for all Australian Government entities	11
Audit findings.....	13
1. Background	14
Introduction	14
Previous audits of entities' cyber security resilience	15
Rationale for undertaking the audit.....	15
Audit approach.....	15
2. Cyber security risk management frameworks	20
Do entities have a fit for purpose cyber security risk management framework?.....	20
Have entities met the requirements of their cyber security risk management framework?	25
3. Alignment with the Information Security Manual's risk mitigation strategies.....	28
Have entities implemented controls that would be in line with the Top Four cyber security risk mitigation strategies?.....	29
Have entities implemented controls that would be in line with the four non-mandatory strategies in the Essential Eight?.....	32
4. Cyber security resilience	37
Do entities have a cyber resilience culture?	37
Are entities cyber resilient?	42
How do entities' cyber security arrangements compare to those of non-corporate Commonwealth entities?.....	46
Appendices	49
Appendix 1 Entity responses	50
Appendix 2 Recommendations and implementation status from Joint Committee of Public Accounts and Audit Report 467: Cybersecurity Compliance (2017)	54
Appendix 3 Grading schemes.....	57
Appendix 4 Australia's Cyber Security Strategy	60

Summary and recommendation

Background

1. The Australian Government's ability to effectively and efficiently deliver its functions relies on government entities prioritising information security. If government information systems can be accessed by intruders, this could compromise the financial and identity security of individuals and the commercial interests of corporations. A secure cyberspace supports online activities for individuals, business and the public sector. Cyber resilience is an entity's ability to continue providing services while deterring and responding to cyber intrusions. Cyber resilience also reduces the likelihood of cyber intrusions that threaten Australians' privacy and Australia's social, economic and national security interests.

2. The *Protective Security Policy Framework* is administered by the Attorney-General's Department to assist Australian Government entities protect their people, information and assets, at home and overseas. Non-corporate Commonwealth entities are required to apply the *Protective Security Policy Framework*. While cyber security is a strategic priority for the Australian Government, it is not mandatory for government business enterprises and corporate Commonwealth entities to apply the *Protective Security Policy Framework*. Accordingly it is better practice for such entities to implement the Top Four and other Essential Eight mitigation strategies in the *Australian Government Information Security Manual* (Information Security Manual).¹

3. Since 2013–14 when the Information Security Manual became mandatory policy for non-corporate Commonwealth entities, the Auditor-General has tabled four performance audits in the Parliament that assessed the cyber security resilience of 14 such entities.² The audits identified that only four entities (29 per cent) had complied with mandatory government requirements for information security, and that the regulatory framework had not driven sufficient improvement in cyber security.

4. Three corporate entities were included in this audit: Australian Postal Corporation (Australia Post) and ASC Pty Ltd (ASC), both government business enterprises; and the Reserve Bank of Australia (Reserve Bank), a corporate Commonwealth entity. These entities were selected based on the character and sensitivity of the information collected, stored and reported — including that the entities manage critical infrastructure or systems of national interest.

Rationale for undertaking the audit

5. Despite the importance of cyber security in safeguarding the Australian Government's digital information, there has been ongoing low levels of cyber resilience of non-corporate Commonwealth entities and weaknesses in the regulatory framework for ensuring compliance with mandatory cyber security strategies. This audit was undertaken to enable comparison with government business enterprises and corporate Commonwealth entities, and provide

1 The Top Four strategies are application whitelisting, patching applications, patching operating systems, and restricting administrative privileges. The non-mandatory Essential Eight strategies are configuring Microsoft Office macros, user application hardening, multi-factor authentication, and daily backup of systems and data.

2 Auditor-General Report No.50 2013–14 *Cyber Attacks: Securing Agencies' ICT System*; Auditor-General Report No.37 2015–16 *Cyber Resilience*; Auditor-General Report No.42 2016–17 *Cybersecurity Follow-up Audit*; and Auditor-General Report No.53 2017–18 *Cyber Resilience*.

information to help strengthen the regulatory framework and improve cyber resilience of Commonwealth entities. In line with the requirements for performance audit of government business enterprises under the *Auditor-General Act 1997*, the Joint Committee of Public Accounts and Audit provided approval for the Australian National Audit Office (ANAO) to examine the cyber resilience of Australia Post and ASC.

Audit objective and criteria

6. The audit objective was to assess the effectiveness of the management of cyber security risks by Australia Post, ASC and the Reserve Bank.
7. To form a conclusion against this objective, the ANAO adopted three high-level criteria:
 - Have entities managed cyber security risks in line with their own risk arrangements?
 - Have entities managed cyber security risks in line with key aspects of the Information Security Manual?
 - Do entities have a culture of cyber security resilience?

Conclusion

8. The Reserve Bank and ASC have effectively managed cyber security risks. Australia Post has not effectively managed cyber security risks, and should continue to implement its cyber security improvement program and key controls across all its critical assets to enable cyber risks to be within its tolerance level.

9. All three entities have a fit for purpose cyber security risk management framework. ASC and the Reserve Bank have met the requirements of their respective frameworks by implementing the specified information and communications technology (ICT) controls that support desktop computers, ICT servers and systems. Australia Post has not met the requirements of its framework, having not implemented all specified key controls.

10. The Reserve Bank and ASC have implemented controls in line with the requirements of the Information Security Manual, including the Top Four and other mitigation strategies in the Essential Eight. Australia Post has not fully implemented controls in line with either the Top Four or the four non-mandatory strategies in the Essential Eight.

11. The Reserve Bank and ASC are cyber resilient, with high levels of resilience compared to 15 other entities audited over the past five years. Australia Post is not cyber resilient but is internally resilient, which is similar to many of the previously audited entities. The Reserve Bank has a strong cyber resilience culture, ASC is developing this culture, and Australia Post is working towards embedding a cyber resilience culture within its organisation.

Supporting findings

Cyber security risk management frameworks

12. All three entities have a fit for purpose cyber security risk management framework. They each have enterprise-wide risk management arrangements that incorporate cyber security, and specific frameworks for managing cyber security risks appropriate to their operations. Each specific framework either includes the Information Security Manual or incorporates elements of

it, with Australia Post and the Reserve Bank also adopting aspects of recognised national and international cyber security frameworks applicable to their industry and regulatory environment. The Reserve Bank has fully established all six assessed risk management and governance arrangements for cyber security. Australia Post and ASC have established three of the six arrangements and partially or largely established the other three arrangements.

13. The Reserve Bank and ASC have met the requirements for implementing ICT controls contained in their cyber security risk management framework. Australia Post has not met the requirements for ICT controls in its framework, having not implemented all specified key controls, and as a result has rated the overall cyber risk as significantly above its defined tolerance level.

Alignment with the Information Security Manual risk mitigation strategies

14. The Reserve Bank and ASC have implemented controls in line with the requirements for the Top Four mandatory cyber security risk mitigation strategies of the Information Security Manual. Australia Post has implemented two of the Top Four mitigation strategies: patching ICT applications and minimising privileged user access.

15. ASC and the Reserve Bank have implemented controls in line with all four non-mandatory mitigation strategies in the Essential Eight. Australia Post has implemented controls for one of those mitigation strategies — daily backups of data. All three entities have implemented mitigation strategies beyond the requirements of the Essential Eight, such as the Reserve Bank using machine learning and analytics to detect cyber threats.

Cyber security resilience

16. The three entities are at different stages in embedding a cyber resilience culture. The Reserve Bank has a strong cyber resilience culture, having established all 13 assessed behaviours and practices in the areas of cyber security governance and risk management, roles and responsibilities, technical support and monitoring compliance. ASC is developing a cyber resilience culture, having embedded seven of the assessed behaviours and practices and working to more fully establish the other six cyber security behaviours and practices within its business processes. While having embedded eight of the 13 assessed behaviours and practices, Australia Post has not systematically managed cyber risks, including not assessing the effectiveness of controls applied outside its specified cyber security risk management framework. Nevertheless, Australia Post is working towards embedding a cyber resilience culture.

17. The Reserve Bank and ASC are cyber resilient as they have met the requirements of their fit for purpose cyber security risk management frameworks. Australia Post is not cyber resilient as it has not met the requirements of its own framework. The Reserve Bank and ASC are also cyber resilient under the requirements of the Information Security Manual, as they have implemented the Top Four cyber security risk mitigation strategies and have effective ICT general controls for logical access and change management. Accordingly, the two entities have a high level of protection from internal and external cyber security threats. Australia Post is not cyber resilient under the requirements of the Information Security Manual, but is internally resilient with effective ICT general controls in place for managing logical access and change processes.

18. The Reserve Bank and ASC respectively had the highest and equal third highest level of cyber resilience of 17 entities examined by the ANAO over the past five years. Australia Post was not cyber

resilient, which was similar to many of the previously audited entities. The small number of government business enterprises and corporate Commonwealth entities assessed (three) means it is not possible to draw conclusions as to the relative level of cyber resilience of corporate compared to non-corporate Commonwealth entities.

Recommendation

Recommendation no. 1
Paragraph 2.28 Australia Post conducts risk assessments for all its critical assets where it has not already done so and takes immediate action to address any identified extreme risks to those assets and supporting networks and databases.

Australia Post: *Agreed.*

Summary of entity responses

19. Summary responses from Australia Post, ASC and the Reserve Bank are provided below, with the full responses at Appendix 1.

Australian Postal Corporation

As a government business enterprise operating in a number of competitive markets (including parcel services, government services, financial services, identity services and retail services), Australia Post conducts its complex business operations in a highly competitive commercial environment, maintaining both community and commercial obligations. We are committed to upholding the security and integrity of the assets and information we maintain.

Australia Post agrees with Recommendation no. 1. Australia Post has clear oversight of its critical asset infrastructures and has prioritised actions under a program of work already underway to address this recommendation. This will involve conducting risk assessments for critical assets not yet assessed, updating assessments for those already assessed, and taking immediate action to address any concerns that are identified. Monitoring of the implementation of this program of work will be managed through our information security risk management and compliance programs, and will be reported to senior management and our Board, through its Audit & Risk Committee.

Australia Post notes that it has been assessed as 'Internally Resilient' under the grading scheme developed by the Australian National Audit Office and applied in the Report. In our view that determination reflects the significant volume of resources and effort Australia Post has already committed to developing its cyber resilience, but that there is still work to be done to move towards, and maintain, a high level of external resilience.

Australia Post maintains a high level of cyber resilience across its critical platforms and systems supporting government, identity and financial services – a number of which have received external accreditation against the *Australian Government Information Security Manual* (Manual).

Australia Post is not required to apply or comply with the Manual or its Top Four mitigation strategies, but has voluntarily chosen to incorporate aspects of the Manual into its cyber security framework – together with other industry-leading frameworks such as the National Institute of Standards and Technology Cybersecurity Framework – as a matter of best practice.

Australia Post is committed to ensuring the security and integrity of its information systems, and to deterring and responding to cyber intrusions. Our continued vigilant focus on the further

implementation of our cyber security risk management framework, and on protecting the integrity and security of our systems, will assist in the preservation of a strong framework of cyber resilience for the benefit of our employees, customers and the Australian community.

ASC Pty Ltd

ASC agrees with the findings in the report with regard to ASC and is pleased with the ANAO determination that ASC is cyber resilient. ASC will use the detail contained in the report to further strengthen those areas where opportunities to improve have been highlighted by the ANAO audit team.

ASC would like to express our appreciation of the manner in which the ANAO audit team conducted the audit with the audit activities providing ASC with a thorough and independent review and assessment of our cyber security implementation and posture. ASC believes that both parties exited from the audit with new learnings that will assist us both in future activities around cyber security.

Reserve Bank of Australia

The Reserve Bank of Australia (RBA) agrees with the findings in the report and that the report is an accurate assessment of our cyber resilience.

The RBA will continue to align with the security controls outlined in the *Australian Government Information Security Manual* and relevant industry security standards as part of our efforts to maintain a strong financial system for all Australians. The RBA is committed to ensuring that we are a cyber-resilient organisation and we will continue to adapt our security strategy to the changing cyber landscape.

Key messages from this audit for all Australian Government entities

20. Below is a summary of key messages, including instances of good practice, identified in this audit that may be relevant for the operations of other Commonwealth entities. Also, Chapter 4 of this report includes lists of behaviours and practices identified in this and previous ANAO audits that, if implemented, may improve the level of cyber resilience of Commonwealth entities.

Governance and risk management

- In establishing specific risk management frameworks for cyber security, the three audited government business enterprises and corporate Commonwealth entities adopted mitigation strategies and controls from the *Australian Government Information Security Manual*, despite not being mandated to do so. The Reserve Bank and Australia Post went further and adopted aspects of recognised national and international cyber security frameworks applicable to their industry or regulatory environments.
- Where controls required within a cyber security framework are not being met, entities such as the Reserve Bank and ASC have undertaken a risk assessment to develop mitigating controls, which have proven effective in meeting the intent of the specified controls. Entities can draw on expertise in the Australian Government (such as the Australian Cyber Security Centre) and the private sector for assistance in strengthening cyber security controls.

- Cyber resilience requires more than entities being compliant with relevant risk management frameworks and controls. The Reserve Bank has embedded behaviours and practices within its organisation that contribute to a strong cyber resilience culture. ASC has demonstrated a positive attitude to managing cyber risks and an open approach to continuous improvements to cyber security processes and practices.

Audit findings

1. Background

Introduction

1.1 The Australian Government's ability to effectively and efficiently deliver its functions relies on government entities prioritising information security. If government information systems can be accessed by intruders, this could compromise the financial and identity security of individuals and the commercial interests of corporations.³ It could also compromise national security, and diminish the Government's reputation and the willingness of individuals and organisations to share their information with the Government.⁴

1.2 A secure cyberspace supports online activities for individuals, business and the public sector. Cyber resilience is an entity's ability to continue providing services while deterring and responding to cyber intrusions. Cyber resilience also reduces the likelihood of cyber intrusions that threaten Australians' privacy and Australia's social, economic and national security interests.

1.3 The *Protective Security Policy Framework* is administered by the Attorney-General's Department to assist Australian Government entities to protect their people, information and assets, at home and overseas. Under the *Public Governance, Performance and Accountability Act 2013*, non-corporate Commonwealth entities are required to apply the *Protective Security Policy Framework* as it relates to their risk environment. Since April 2013, the *Protective Security Policy Framework* has stated that non-corporate Commonwealth entities must mitigate common and emerging cyber threats. The *Protective Security Policy Framework* mandates non-corporate Commonwealth entities implementing four strategies that are detailed in the *Australian Government Information Security Manual* (Information Security Manual) published by the Australian Signals Directorate.⁵ The strategies have been referred to as the 'Top Four' and address: application whitelisting; patching applications; restricting administrative privileges; and patching operating systems. The strategies are described in Chapter 3 of this report.

1.4 Despite cyber security being a strategic priority for the Australian Government and an increasing risk across government entities⁶, it is not mandatory for government business enterprises and corporate Commonwealth entities to apply the requirements under the *Protective Security Policy Framework*. The framework currently represents better practice for such entities. Those entities are only required to apply the *Protective Security Policy Framework* if they are

3 Government networks can be targeted for a cyber intrusion by cybercriminals, issue-motivated groups and individuals, and state-sponsored adversaries. The Australian Cyber Security Centre has reported extensive foreign state-sponsored activity against Australian Government and private sector networks that support economic, foreign policy and national security objectives.

Australian Cyber Security Centre, *Threat Report 2017* [Internet], ACSC, Australia, 2017, available from https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf [accessed 29 January 2019].

4 Australian National Audit Office, *Insights from reports tabled April to June 2018*, [Internet], available from <https://www.anao.gov.au/work/audit-insights/insights-reports-tabled-april-june-2018> [accessed 8 April 2019].

5 Australian Signals Directorate, *Australian Government Information Security Manual* [Internet], [Internet], ASD, Australia, 2019, available from <https://acsc.gov.au/infosec/ism/index.htm> [accessed 5 February 2019].

6 Department of the Prime Minister and Cabinet, *Australia's Cyber Security Strategy* [Internet], DPM&C, Australia, 2016, available from <https://www.pmc.gov.au/sites/default/files/publications/australias-cyber-security-strategy.pdf> [accessed 10 May 2019].

directed to comply under a government policy order under sections 22 or 93 of the *Public Governance, Performance and Accountability Act 2013*. No such orders have been issued to date.

Previous audits of entities' cyber security resilience

1.5 Starting in 2013–14, the Auditor-General has tabled four performance audits in the Parliament that assessed the cyber security resilience of 14 non-corporate Commonwealth entities.⁷ The entities examined in those audits held information across a range of economic, commercial, policy or regulatory, national security, program and service delivery, and corporate activities. The audits identified that only four entities (29 per cent) had complied with mandatory government requirements for information security, and that the regulatory framework had not driven sufficient improvement in cyber security.

1.6 The Australian Parliament's Joint Committee of Public Accounts and Audit (JCPAA) published *Report 467: Cybersecurity Compliance* in October 2017. The report followed a Committee inquiry based on Auditor-General Report No.42 2016–17 *Cybersecurity Follow-up Audit*. The Committee's 10 recommendations and their current status of implementation are shown in Appendix 2. As at April 2019, five recommendations had been implemented (one implemented late), two partly agreed and/or partly implemented and three agreed or partly agreed but not yet implemented. The lack of timely responses to these recommendations is not in line with the JCPAA's statement in Report 467 that 'as a strategic priority, it is crucial that Commonwealth entities be accountable to the Australian Parliament on cybersecurity'.⁸

Rationale for undertaking the audit

1.7 Despite the importance of cyber security in safeguarding the Australian Government's digital information, there has been ongoing low levels of cyber resilience of non-corporate Commonwealth entities and weaknesses in the regulatory framework for ensuring compliance with mandatory cyber security strategies. This audit was undertaken to enable comparison with government business enterprises and corporate Commonwealth entities, and provide information to help strengthen the regulatory framework and improve cyber resilience of Commonwealth entities. In line with the requirements for performance audit of government business enterprises under the *Auditor-General Act 1997*, the JCPAA provided approval for the Australian National Audit Office (ANAO) to examine the cyber resilience of the Australian Postal Corporation and ASC Pty Ltd.

Audit approach

1.8 Of 79 Australian Government business enterprises and corporate Commonwealth entities, three entities were selected for this audit: Australian Postal Corporation (Australia Post) and ASC Pty Ltd (ASC), both government business enterprises; and the Reserve Bank of Australia (Reserve Bank), a corporate Commonwealth entity.

7 Auditor-General Report No.50 2013–14 *Cyber Attacks: Securing Agencies' ICT System*; Auditor-General Report No.37 2015–16 *Cyber Resilience*; Auditor-General Report No.42 2016–17 *Cybersecurity Follow-up Audit*; and Auditor-General Report No.53 2017–18 *Cyber Resilience*.

8 Joint Committee of Public Accounts and Audit Report 467 (p. 15), [Internet], available from https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/Completed_inquiries [accessed 6 February 2019].

1.9 The selection process for this audit included an assessment of each entity against the following factors:

- type of information held by the entity;
- type of services provided by the entity; and
- whether the entity manages critical infrastructure or systems of national interest, such as those relating to financial services and information technology, which continue to be a focus for cybercriminals.

1.10 Table 1.1 outlines the key information collected, stored and used by Australia Post, ASC and the Reserve Bank.

Table 1.1: Audited entities' information holdings and service characteristics

Entity	Economic or commercial information	Citizens' personal information	National security or critical infrastructure	Program and service delivery	Policy or regulatory body
Australia Post	✓	✓	✓	✓	—
ASC	✓	—	✓	✓	—
Reserve Bank	✓	—	✓	✓	✓

Source: ANAO analysis.

Australia Post

1.11 The Australian Postal Corporation (Australia Post) operates under the *Australian Postal Corporation Act 1989*. It is a government-owned business required to earn a commercial rate of return and meet specified community service obligations.⁹ The Australian Government is Australia Post's only shareholder through the Minister for Communications and the Minister for Finance. Australia Post's Chair is selected by the Minister for Communications and the Minister for Finance.¹⁰

1.12 Australia Post provides direct services to its customers in the following areas:

- a national retail network;
- mail delivery, parcel delivery and shipping services, domestically and internationally;
- financial transactions and payment services, domestically and internationally;
- identity verification services, including for passports, licence renewals and proof of age cards; and

9 Australia Post is an independent, commercial entity that operates in a highly competitive environment for many of its services. It does not receive any government funding to support its operations, rather, it returns funds to the Commonwealth in the form of dividends and taxes.

10 Under the *Australian Postal Corporation Act 1989* subsection 73(1), the Governor-General appoints directors on the nomination of the Minister. The Chair is a director. The Board Charter indicates that the Chair is selected by shareholder Ministers.

- data management and logistics services, for business and government.¹¹

1.13 Australia Post provides financial services through a network of more than 4000 post offices, including over 2500 post offices in rural and remote Australia. It also manages an extensive physical operational asset base and the provision of these services is supported by over 1500 applications. Australia Post directly employs around 35,000 people across its integrated delivery, logistics, retail and eCommerce network.¹²

ASC

1.14 ASC (formerly known as the Australian Submarine Corporation) was established as a joint venture in 1985 to design and build a new fleet of submarines for the Royal Australian Navy. ASC has been a wholly government owned business since 2000. ASC is a proprietary company limited by shares registered under the *Corporations Act 2001* — all the shares issued in the capital of ASC are owned by the Commonwealth of Australia, represented by the Minister for Finance. The Chair of the ASC Board is appointed by the Finance Minister. In 2017–18, ASC had approximately 2200 employees.

1.15 ASC provides the following services:

- sustainment for the current fleet of Collins Class submarines, which includes maintenance, repairs and design upgrades;
- training services for submariners;
- building the Hobart Class air warfare destroyers; and
- building the lead and second Arafura Class offshore patrol vessels.

Reserve Bank

1.16 The Reserve Bank was established under the *Reserve Bank Act 1959* as Australia's central bank. The Reserve Bank is a statutory authority with the power to make monetary and banking policy. The Reserve Bank is governed by two boards: the Reserve Bank Board and the Payments System Board. In June 2018, the Reserve Bank had 1362 employees.

1.17 The Reserve Bank is responsible for the following areas and objectives:

- setting the interest rate on overnight loans in the money market ('cash rate') through monetary policy;
- setting a target for the cash rate through financial market operations;
- maintaining the stability of the financial system through mitigating and responding to major financial disturbances;
- overseeing Australia's payment system and regulating the infrastructure supporting the clearing and settlement of transactions in financial markets;
- providing a range of banking services to the Australian Government and overseas central banks; and

11 Refer to paragraph 1.21 for the specific information systems selected for audit coverage for each of the entities.

12 Counting the thousands of people Australia Post employs indirectly — including licensed post office operators, community postal agents and delivery drivers — its extended workforce exceeds 70,000.

- all aspects of the production, issuance, security of, and the maintenance of confidence in, Australian banknotes.

Audit objective, criteria and scope

1.18 The audit objective was to assess the effectiveness of the management of cyber security risks by Australia Post, ASC and the Reserve Bank.

1.19 To form a conclusion against this objective, the ANAO adopted three high-level criteria:

- Have entities managed cyber security risks in line with their own risk arrangements?
- Have entities managed cyber security risks in line with key aspects of the Information Security Manual?
- Do entities have a culture of cyber security resilience?

1.20 The scope included:

- assessing whether the entities met the requirements of their chosen cyber security risk management framework, including assessing the cyber security controls that were implemented;
- assessing whether the entities' management of cyber security risks aligned with key aspects of the Information Security Manual, as government business enterprises and corporate Commonwealth entities are not required to apply the *Protective Security Policy Framework*; and
- similar to the previous audit¹³ in the series, assessing entities' cyber security culture, that is, the shared organisational attitudes, values and behaviours regarding cyber risks that complement the technical security solutions for managing cyber risks.

1.21 The assessment was performed on the corporate platform and selected systems that were rated as critical by the entities. The selected systems were: the Reserve Bank's Information and Transfer System¹⁴; ASC's Enterprise Resource Planning System¹⁵; and Australia Post's Corporate Data Warehouse and eParcel application.¹⁶

1.22 The selected systems did not include: financial and human resource management information systems, which were non-critical; security sensitive and classified networks within

13 Auditor-General Report No.53 2017–18 *Cyber Resilience*.

14 The Reserve Bank's Information and Transfer System provides the infrastructure to assist banks and other approved institutions in settling their payment obligations in a safe and efficient manner. The System's platform also supports other payment services and systems, such as the Fast Settlement Service and New Payments Platform.

15 The Enterprise Resource Planning System CONTROL application supports all ASC's key business areas and provides support to other business applications. CONTROL is the major application that resides on the unclassified network and holds commercially sensitive data, such as project material and financial information.

16 The Corporate Data Warehouse is a central store of data that supports Australia Post's development and production of analytical and operational reports, which are used to support activities ranging from the provision of external customer services to operational decision making. The warehouse holds data on retail transactions, operations and logistics, human resources and financial management. The eParcel application supports the transfer of logistics and manifest data between Australia Post and merchants. It facilitates Australia Post's and merchants' ability to electronically manage deliveries throughout the delivery process.

ASC¹⁷; and Australia Post's retail environment or systems supporting government, identity and financial services.¹⁸

1.23 Given the large number of critical applications in these entities, a sample of critical applications was selected to assess each entity's capability of implementing adequate controls for protecting, detecting and responding to cyber threats. The basis for taking this approach is that entities would prioritise and invest in the protection of applications and information assets that were critical to their business. The effectiveness of the entities in managing cyber security risks across the selected critical systems would provide an indication of their cyber threat mitigation strategies for other critical systems across the entity. Additionally, a sample of controls were tested from each entity's cyber security framework that were focused on areas that were relevant to mitigating cyber threats, such as system configuration, network security, identity management, and logging and monitoring.

Audit methodology

1.24 In December 2018 and January 2019, the ANAO collected and reviewed documents and tested selected systems in each entity for the period 1 January 2018 to 8 February 2019. Staff were interviewed in all three entities, including executive staff, Board members, and audit and risk committee members.

1.25 During fieldwork for the audit, in December 2018 a new edition of the Information Security Manual was published. Entities' security controls continued to be examined under the 2017 edition during the audit. However, if a control was assessed as inadequate it was also examined under the December 2018 edition of the Information Security Manual to establish if the control was adequate under the new edition.¹⁹ Entities were also asked to describe their response to the new requirements in the Information Security Manual and assess whether those requirements would apply to their cyber security culture.

1.26 The audit was conducted in accordance with the ANAO Auditing Standards at a cost to the ANAO of approximately \$720,000. The team members for this audit were Esther Barnes, Edwin Apoderado, Kelvin Le, Jason Ralston, Carissa Chen, David Ma, David Willis, Bola Oyetunji and Andrew Morris.

17 ASC's classified networks do not interface with unclassified systems and would be less susceptible to cyber attacks given the logical and physical segregation from unclassified systems.

18 Australia Post's corporate environment also stores retail data and the government interfacing systems did not support the majority of Australia Post's business operations.

19 The changes in the Information Security Manual in December 2018 updated and removed certain requirements to reduce duplication, improve guidance and support a risk management culture rather than a compliance culture. There were no material changes to the Essential Eight mitigation strategies (described in Chapter 3).

2. Cyber security risk management frameworks

Areas examined

This chapter examines whether the entities have established fit for purpose cyber security risk management frameworks and managed cyber security risks according to those frameworks.

Conclusion

All three entities have a fit for purpose cyber security risk management framework. ASC and the Reserve Bank have met the requirements of their respective frameworks by implementing the specified information and communications technology (ICT) controls that support desktop computers, ICT servers and systems. Australia Post has not met the requirements of its framework, having not implemented all specified key controls.

Areas for improvement

This chapter has one recommendation aimed at Australia Post taking timely action to address cyber security risks associated with its critical assets (paragraph 2.28).

Do entities have a fit for purpose cyber security risk management framework?

All three entities have a fit for purpose cyber security risk management framework. They each have enterprise-wide risk management arrangements that incorporate cyber security, and specific frameworks for managing cyber security risks appropriate to their operations. Each specific framework either includes the *Australian Government Information Security Manual* or incorporates elements of it, with Australia Post and the Reserve Bank also adopting aspects of recognised national and international cyber security frameworks applicable to their industry and regulatory environment. The Reserve Bank has fully established all six assessed risk management and governance arrangements for cyber security. Australia Post and ASC have established three of the six arrangements and partially or largely established the other three arrangements.

Design of entities' cyber security risk management frameworks

2.1 The audit examined each entity's approach to cyber security as part of their overall management of risks as well as the specific risk management frameworks in place for managing cyber security risks. Table 2.1 summarises the entities' risk management frameworks for cyber security.

Table 2.1: Entities' cyber security risk management frameworks

Entity	Summary of the cyber security risk management framework
Australia Post	<p>Incorporates aspects of the following frameworks:</p> <ul style="list-style-type: none"> • <i>Australian Government Information Security Manual</i>; • National Institute of Standards and Technology (NIST), <i>Cybersecurity Framework</i>^a; • <i>ISO/IEC 27002 Information technology — Security techniques — Code of practice for information security controls</i>; and • Payment Card Industry Data Security Standard.

Entity	Summary of the cyber security risk management framework
ASC	Incorporates the <i>Australian Government Information Security Manual</i> .
Reserve Bank	Incorporates the <i>Australia Government Information Security Manual</i> and aspects of the following frameworks: <ul style="list-style-type: none"> • ISO/IEC 27000 suite of standards for information security management systems; • <i>Protective Security Policy Framework</i>; • Australian Prudential Regulation Authority, <i>Practice Guide CPG 234 — Management of Security Risk in Information and Information Technology</i>; and • Standards for the Society for Worldwide Interbank Financial Telecommunication (SWIFT).

Note a: The NIST Cybersecurity Framework, developed in the United States in 2014 in response to a Presidential Executive Order, provides guidance to help organisations better understand, manage and reduce cyber security risks.

Source: ANAO analysis of entity documents.

2.2 In establishing their cyber security risk management frameworks, all three entities assessed various existing international and national frameworks, including the *Australian Government Information Security Manual* (Information Security Manual). Despite the Top Four mitigation strategies not being mandatory for these entities (as discussed in Chapter 1), all three entities included these strategies in their cyber security risk management frameworks. All three entities' frameworks also covered the additional four mitigation strategies in the Essential Eight (as discussed in Chapter 3). The cyber security risk management frameworks of the Reserve Bank and Australia Post also incorporate national and international standards.

2.3 The Reserve Bank reviewed its cyber security risk management framework in 2016, engaging an external firm to assess the most commonly used IT industry frameworks and identify potential controls to complement its prevailing protection mechanisms based on the Information Security Manual. The review was completed in 2016 and recommended that the Reserve Bank define a set of principles based on commonly used frameworks²⁰ to address risks not covered by the Information Security Manual. The review suggested a risk-based approach to implementing elements of ISO 27001, the most commonly used framework by central banks, and also elements of other frameworks. Accordingly, the Reserve Bank implemented ISO 27001 in conjunction with the Information Security Manual, and other frameworks as set out in Table 2.1. The Reserve Bank also participated in the SWIFT Customer Security Program, which seeks to establish a security baseline for the entire financial community, and fosters transparency of security compliance across participants.

2.4 ASC adopted the Information Security Manual as its security framework, which is an appropriate approach given the nature of its operations and membership within the Defence

²⁰ The review examined the following frameworks: Control Objectives for Information and Related Technology (COBIT) 5; International Organization for Standardization (ISO) 27001; Information Technology Infrastructure Library (ITIL) v3; National Institute of Standards and Technology (NIST) Cybersecurity Framework; and NIST Special Publication (SP) 800-53 revision 4.

Industry Security Program.²¹ The program requires members to comply with the Defence Security Principles Framework, which includes a requirement to comply with the *Protective Security Policy Framework* and Information Security Manual.

2.5 Similar to the Reserve Bank, Australia Post has established a security framework that incorporates requirements from the Information Security Manual, NIST, and other frameworks as set out in Table 2.1. Australia Post’s security standards include certain controls from each framework and were selected based on risk and applicability to Australia Post’s business and environment.

Effectiveness of entities’ risk management and governance arrangements for cyber security

2.6 Table 2.2 shows the effectiveness of the three entities’ risk management and governance arrangements for cyber security. The assessment is based on criteria developed by the ANAO in the previous cyber resilience audit report.²²

Table 2.2: Effectiveness of entities’ risk management and governance arrangements for cyber security

Areas assessed for risk management and governance arrangements	Australia Post	ASC	Reserve Bank
Enterprise-wide governance arrangements	◆	◆	◆
Information security roles assigned and responsibilities communicated	◆	◆	◆
ICT security incorporated into strategy, planning and delivery of services	◆	▲	◆
ICT operational staff understand the vulnerabilities and cyber threats to the system	▲	▲	◆
Integrated and documented architecture for data, systems and security controls	▲	▲	◆
Systematic approach to managing cyber risks, including assessments of the effectiveness of controls and security awareness training	▲	◆	◆
<p>Key:</p> <p>◆ Established. Arrangements in place and maintenance is part of business processes including monitoring and taking corrective action as required.</p> <p>▲ Partially or largely established. Some key elements of the arrangements have not been established.</p> <p>■ Arrangements have not been established.</p>			

Source: ANAO analysis.

21 Entities that supply goods and services to the Department of Defence or work on classified information or assets are required to hold an appropriate level of Defence Industry Security Program membership. This membership provides entities with information, services and support to help them manage security risks and protect sensitive information and assets in line with the Department of Defence’s security requirements; Department of Defence, *Defence Security Principles Framework* [Internet], 2018, [Internet], available from http://www.defence.gov.au/DSVS/_Master/resources/DSPF-Unclass-Version.pdf [accessed 24 April 2019].

22 Auditor-General Report No.53 2017–18 *Cyber Resilience*, p. 45.

2.7 Table 2.2 shows that the Reserve Bank has all six assessed risk management and governance arrangements in place to support its management of cyber security risks. Australia Post and ASC both have established three of these arrangements and partially or largely established the other three arrangements, where some key elements have not been implemented.

Enterprise-wide governance arrangements

2.8 All three entities have an Enterprise Risk Management Framework that was supported by risk management plans or policies. The frameworks were aligned with the Australian and New Zealand standard (AS/NZS ISO 31000:2009) for the development of risk management frameworks and programs.²³ In all three entities, cyber risks were identified and managed with other types of business risks on entity risk registers. In addition, the Reserve Bank has published a Risk Appetite Statement that covers cyber attacks on its systems or networks that states: 'The Bank has a very low appetite for damage to Bank assets from threats arising from malicious attacks'.²⁴ Australia Post also has a Risk Appetite Statement that states it supports: 'a highly secure environment and will not tolerate data security incidents resulting in material theft, loss or corruption of business or confidential internal and customer data.' ASC does not have a Risk Appetite Statement.

2.9 All three entities have governance arrangements in place involving senior executives and board level committees, which meet regularly to consider and manage cyber security risks. The committees are supported by adequate monitoring and reporting on cyber security matters.

Information security roles assigned and responsibilities communicated

2.10 Clearly defined information security roles are assigned either to individuals or committees in all three entities. All three entities have appointed security advisors, such as a Chief Information Security Officer, to assist more senior staff or to assist with the daily delivery of information security requirements.

ICT security incorporated into strategy, planning and delivery of services

2.11 Australia Post and the Reserve Bank have effectively incorporated ICT security into their strategies, plans and activities to deliver services. Specifically, Australia Post and the Reserve Bank include ICT security arrangements in strategic plans, business planning processes, project management arrangements, and financial management processes.

2.12 ASC's strategic plans identify cyber security as a risk for its business. ASC uses governance arrangements for cyber security to involve senior executives in further developing its cyber security capability. The Chief Information Security Officer is leading the implementation of capability development activities. There is currently no long-term, approved plan in place for additional investments in cyber security. Further investments in cyber security are managed as part of ASC's business planning process. ASC includes its ICT security budgets and expenditure in its financial management processes. ASC's information security strategy that was developed in 2016 has come to an end. ASC advised in May 2019 that the business case for the Digital Transformation Program,

23 Corporate Commonwealth entities are not required to comply with the Commonwealth Risk Management Policy, but they should review and align their risk management frameworks and systems with this policy as a matter of good practice.

24 Reserve Bank of Australia, *Risk Appetite Statement* [Internet], RBA, Australia, 2018, available from <https://www.rba.gov.au/about-rba/our-policies/risk-appetite-statement.html> [accessed 29 April 2019].

which encompasses a new IT Strategy, had been completed and was being progressed through the relevant approval processes.

ICT operational staff understand the vulnerabilities and cyber threats to the system

2.13 The Reserve Bank has comprehensive arrangements in place to support ICT operational staff understand cyber threats to the ICT systems that support corporate and service operations. The Reserve Bank primarily uses in-house operational staff to support its ICT systems. All ICT operational staff, and contract staff working on-site, are required to complete a security induction. Activities to inform ICT staff about potential cyber threats to the Reserve Bank's systems include daily, weekly and monthly briefings and forums among ICT security and operational teams.

2.14 Australia Post and ASC mostly use in-house operational staff to support their ICT systems. These staff and external contractors are required to complete a security induction process. Both entities encourage their ICT security staff to identify and complete training that supports their roles and responsibilities, although there is no mandatory cyber security training requirement for staff in the ICT security teams. Both entities' ICT security teams undertake a range of in-house activities to identify potential vulnerabilities, and regularly discuss the results with ICT operational staff. Although Australia Post provided vulnerability reports and risk assessments, these did not cover all critical systems. ASC does not document all the vulnerabilities identified from its assessments.

2.15 Australia Post and the Reserve Bank actively contribute to external industry and professional forums that enable the sharing of information on cyber security. ASC participates in a limited number of external forums as a means of obtaining updates and increasing its awareness of cyber security vulnerabilities and cyber security threats.

Integrated and documented architecture for data, systems and security controls

2.16 The Reserve Bank has identified, and clearly described and documented, its critical ICT assets. The Reserve Bank has also documented the threats, risks and mitigations to those assets. Incident response plans and business continuity plans include the priority of services to be maintained or restored in the entity.

2.17 ASC has not separately identified critical ICT assets, instead treating all information assets as critical. ASC has documented the threats, risks and mitigations that would be required under a generic threat scenario to the critical information network that was examined by the ANAO.²⁵ Further work would be required by ASC to develop tailored threat and risk profiles for specific information assets. ASC has not updated its information security strategy since 2016 and is progressing the approval of a new strategy (as discussed in paragraph 2.12). Plans for incident response and business continuity identify the priority of services that need to be maintained or restored by ASC.

2.18 While Australia Post has identified its critical ICT assets, it has not documented the threats, risks and mitigations against all critical assets. Further work is required by Australia Post to validate the level of exposure and protection required across its critical assets. Australia Post has scheduled initiatives to progress risk and threat assessments for all critical assets. Australia Post has also established plans to respond to incidents and business continuity events, including the priority of services to be maintained or restored.

25 As explained in Chapter 1, the audit examined a selection of the critical information systems in each entity.

Systematic approach to managing cyber risks, including assessments of the effectiveness of controls and security awareness training

2.19 ASC and the Reserve Bank have systematic approaches to managing cyber security risks that include, but are not limited to:

- implementing a baseline of prescribed controls, that are regularly monitored and assessed for effectiveness;
- the sanctioned use of additional mitigation strategies when necessary;
- performing penetration tests of ICT systems, networks or applications to find security vulnerabilities that an attacker could exploit; and
- delivering security awareness training for all entity staff, such as phishing simulations to try to gather personal information using deceptive emails and websites.

2.20 Similarly, Australia Post has defined an approach to managing cyber security risks that includes security awareness training. However, it has not implemented baseline²⁶ controls on all critical assets or undertaken recent assessments to determine the effectiveness of alternative cyber security controls. Accordingly, it has not been systematic in managing cyber risks.

Have entities met the requirements of their cyber security risk management framework?

The Reserve Bank and ASC have met the requirements for implementing ICT controls contained in their cyber security risk management framework. Australia Post has not met the requirements for ICT controls in its framework, having not implemented all specified key controls, and as a result has rated the overall cyber risk as significantly above its defined tolerance level.

2.21 The ANAO reviewed a sample of controls supporting desktop computers, ICT servers and systems in Australia Post, ASC and the Reserve Bank. As all three entities' frameworks for managing cyber security risks included elements of the Information Security Manual, there was overlap in the ANAO's testing of these frameworks reported in this chapter and of controls under the Information Security Manual reported in Chapter 3. There was complete overlap for ASC that adopted the Manual, considerable overlap for the Reserve Bank, but greater variation in testing for Australia Post.²⁷

2.22 In respect of the Reserve Bank, the ANAO reviewed eight of 16 mandatory SWIFT controls, some of which were aligned to the Top Four strategies. The sampled controls covered the SWIFT principles relating to reducing attack vulnerabilities, preventing compromise of credentials, segregating privileges and detecting anomalous activity. For Australia Post, the ANAO reviewed two of 13 Tier 1 Cyber Security mitigation controls and eight of 189 Information Security Standards controls, which Australia Post had specified in its cyber security risk management framework.²⁸ These controls covered infrastructure and malicious content vulnerability management, security

26 Australia Post's cyber security risk management framework defines a set of mandatory security controls that are required across its platforms, systems and applications. This audit refers to those as 'baseline' controls.

27 As Australia Post's framework included controls from many different frameworks and not predominantly the Information Security Manual, there was more variation in the ANAO testing of controls.

28 The 189 controls were selected from Information Security Standards that specifically related to detection and prevention of cyber threats, such as system configuration, network security, identity management, logging and monitoring.

procedures and tools, system security configuration, identity management, logging and monitoring, and security awareness. For ASC, the ANAO reviewed 65 of 830 Information Security Manual controls that covered access to systems, operating systems and application hardening, system administration and patching, and event logging and monitoring. The 65 controls were selected given their alignment to the requirements of the Essential Eight.

2.23 In ASC and the Reserve Bank, all sampled controls were designed and implemented as specified in their respective cyber security risk management framework. Where mitigating controls were used to supplement mandatory standards in the framework, these were operating effectively. There was some scope for both entities to include more detailed guidance in documentation supporting review and monitoring activities, although the existing entity personnel were adequately skilled and experienced in applying the required procedures. As part of the audit, non-ICT security staff in a wide range of roles in the two entities were interviewed to ascertain whether security awareness activities were available, promoted and attended by staff. Entity staff, at all levels, advised that they were aware of the entity's security programs, cyber security incident and response processes, and how to report suspicious emails.

2.24 All three entities monitor for the presence of cyber security incidents, both internal and external. The ICT security team in each entity is responsible for notifying staff when there is a heightened threat of a cyber security incident. Any incidents are to be investigated by the ICT security team to determine the root causes; after which remediation plans are to be developed and communicated to internal stakeholders. The Reserve Bank was proactive in its approach to security incidents and has implemented mitigation strategies to reduce the risk of incidents occurring. For example, the intelligence function within the ICT security team had identified potential concerns with a ransomware attack (WannaCry), and implemented controls to detect and prevent the threat. Similarly, all entities communicated the concerns of the PageUp breach²⁹ to its staff and provided guidance on how to respond to attacks arising from the breach. All entities also assessed the impact on its environment and where required, extended investigations and discussions to external stakeholders to limit the exposure.

2.25 In Australia Post, only half of the sampled controls (five of 10) were designed and implemented as specified in its cyber security risk management framework. Three of the 10 sampled controls were partly implemented and two controls were not implemented. No approval documentation or risk assessment was available to support the deviation from the framework.

2.26 Australia Post's cyber security framework and controls have been the focus of internal reviews, which highlighted that Australia Post had not fully implemented the security standards in its cyber security risk management framework. Based on the recommendations of the internal reviews, to mitigate cyber security risks Australia Post had implemented controls that are outside its framework. Similar to the findings of Australia Post's internal reviews, the ANAO's analysis found that Australia Post had not fully implemented all key controls specified in its cyber security risk management framework (refer previous paragraph). As discussed in Chapters 3 and 4, the overall

29 PageUp Limited, an online recruitment services organisation, notified its customers about a data incident in which certain information pertaining to staff members, applicants and referees was accessed by an unauthorised third party. The notification was on Friday, 1 June 2018. See [Internet], <https://www.cyber.gov.au/news/pageup-data-incident> [accessed 11 April 2019].

set of mitigating controls implemented have not been sufficient to address cyber security risks. That is, Australia Post's existing controls do not sufficiently mitigate the risks it has identified.

2.27 Australia Post has rated its overall cyber security risk as significantly above its defined risk tolerance level.³⁰ Consequently, in 2018 Australia Post established a cyber security program, 'Securing Tomorrow', which focuses on reducing cyber risks to within its risk tolerance by 2020. The program is a three year program that addresses long-term strategic initiatives. However, to inform 'Securing Tomorrow', Australia Post has not performed risk assessments for all its critical assets³¹, which has limited its visibility of the threats and current controls for those assets.

Recommendation no.1

2.28 Australia Post conducts risk assessments for all its critical assets where it has not already done so and takes immediate action to address any identified extreme risks to those assets and supporting networks and databases.

Australia Post response: *Agreed.*

2.29 *Australia Post agrees with Recommendation no. 1. Australia Post has clear oversight of its critical asset infrastructures and has prioritised actions under a program of work already underway to address this recommendation. This will involve conducting risk assessments for critical assets not yet assessed, updating assessments for those already assessed, and taking immediate action to address any concerns that are identified. Monitoring of the implementation of this program of work will be managed through our information security risk management and compliance programs, and will be reported to senior management and our Board, through its Audit & Risk Committee.*

30 Australia Post's risk rating of 'extreme' was based on its assessment of the consequences of the cyber security risk to its key business functions and the likelihood of the risk eventuating within 12 months.

31 The program includes several initiatives focused on assessing the level of compliance with Australia Post's baseline controls.

3. Alignment with the Information Security Manual's risk mitigation strategies

Areas examined

This chapter examines whether entities have managed their cyber security risks in line with key aspects of the Information Security Manual.

Conclusion

The Reserve Bank and ASC have implemented controls in line with the requirements of the Information Security Manual, including the Top Four and other mitigation strategies in the Essential Eight. Australia Post has not fully implemented controls in line with either the Top Four or the four non-mandatory strategies in the Essential Eight.

Areas for improvement

This chapter has identified strategies and controls for Australia Post to strengthen to be in line with the Top Four and other mitigation strategies in the Essential Eight. ASC and the Reserve Bank could further strengthen some controls for patching applications and operating systems; ASC could also strengthen controls for application whitelisting.

3.1 To safeguard information from cyber security threats, non-corporate Commonwealth entities must implement four mitigation strategies (commonly known as the 'Top Four') from the Information Security Manual (refer paragraph 1.3). The four mitigation strategies, in combination with a further four (non-mandatory) mitigation strategies, form a baseline known as the 'Essential Eight'.

3.2 The four required strategies, of the Essential Eight, are defined in Table 3.1. The remaining four non-mandatory strategies are described later in the chapter in Table 3.3.

Table 3.1: Top Four mandatory mitigation strategies

Mitigation strategy	Why apply the strategy?
To prevent malware delivery and execution	
Application whitelisting	All non-approved applications, including malicious code, are prevented from executing.
Patch applications ^a	Security vulnerabilities in applications can be used to execute malicious code on systems.
To limit the extent of cyber security incidents	
Restrict administrative privileges	Administration accounts are the 'keys to the kingdom'. Adversaries use these accounts to gain full access to information and systems.
Patch operating systems	Security vulnerabilities in operating systems can be used to further the compromise of systems.

Note a: A patch is a piece of software designed to fix problems with, or update, a computer program or its supporting data. Examples of common applications include web browsers, Microsoft Office, Java, Flash and PDF viewers.

Source: Adapted from Australian Cyber Security Centre documents.

3.3 As government business enterprises or corporate Commonwealth entities, it is not mandatory for Australia Post, ASC or the Reserve Bank to implement the Top Four mandatory strategies of the Essential Eight. Nevertheless, each entity addressed the Top Four mitigation

strategies, and the other four strategies in the Essential Eight, in their cyber security risk management frameworks.

3.4 This chapter examines whether the three entities have implemented controls in line with the Top Four and other Essential Eight mitigation strategies in the Information Security Manual, to enable comparisons with previous ANAO audits of cyber security in non-corporate Commonwealth entities (refer Chapter 4). While it was not mandatory for the entities to do so under the *Protective Security Policy Framework*, implementing the Top Four strategies, or elements of them, was necessary to satisfy the requirements of their own cyber security risk management framework.

Have entities implemented controls that would be in line with the Top Four cyber security risk mitigation strategies?

The Reserve Bank and ASC have implemented controls in line with the requirements for the Top Four mandatory cyber security risk mitigation strategies of the Information Security Manual. Australia Post has implemented two of the Top Four mitigation strategies: patching ICT applications and minimising privileged user access.

3.5 Table 3.2 shows the three entities' implementation of the Top Four mitigation strategies. The results, from the application of a standard set of assessment criteria, were aggregated to an overall grade that is described in more detail in Appendix 3.

Table 3.2: Entities' implementation of the Top Four mitigation strategies

Control areas assessed	Assessment results		
	Australia Post	ASC	Reserve Bank
Application whitelisting			
Patching applications			
Patching operating systems			
Restricting administrative privileges			

Key:

	Controls not in place and no dispensation authorised by the Accountable Authority.		Controls in place and meeting control objectives.
	Controls not in place but a dispensation is authorised by the Accountable Authority.		Controls in place and maintenance is part of business processes, including monitoring and taking corrective action as required.
	Controls not in place but entity is actively implementing, with a minimum of design deliverables in evidence.		

Source: ANAO analysis.

3.6 Table 3.2 shows that the Reserve Bank and ASC implemented each of the Top Four mitigation strategies and therefore would have met the mandatory requirement set out in the *Protective Security Policy Framework* (and linked to the Information Security Manual). Australia Post implemented two of the Top Four mitigation strategies.

Application whitelisting

3.7 The purpose of application whitelisting is to protect systems and networks from security vulnerabilities in existing applications, and prevent unauthorised applications from running on ICT systems. One of the Top Four mitigation strategies is application whitelisting for desktops and servers.

3.8 The Reserve Bank and ASC have implemented whitelisting controls in both the desktop and server environments using several methods that were consistent with the Information Security Manual and allowed a balance between the entity's security and business operational needs. ASC does not have procedures for removing whitelisting rules or a process for regularly reviewing whitelisting rules for its Windows desktops and servers other than when new applications were being added.

3.9 ASC and the Reserve Bank have documented application whitelisting strategies, which allowed for exemptions such as when developing, testing and installing applications. ASC requires a risk assessment for exemptions and the Reserve Bank requires mitigating controls to be put in place for exemptions. Both ASC and the Reserve Bank require any changes — additions, modifications, or deletions of applications — from the entity's whitelisting library to be reviewed and approved by the ICT security team.

3.10 Australia Post has no application whitelisting controls in place to block unauthorised applications from executing on its corporate desktop or server environments. Australia Post had assessed the associated risks and determined that application whitelisting controls would not be suitable for operations within particular environments, such as its corporate desktop and server environments. Australia Post advised the ANAO that it has implemented application whitelisting controls supporting its retail³² and deliveries environments. In the absence of application whitelisting controls for its corporate desktop and server environments, Australia Post advised the ANAO that it has implemented some other controls to mitigate risks. However, the ANAO's testing of these mitigating controls found that they were not directly applicable to the threats faced and did not provide sufficient coverage, protection or monitoring of the security vulnerabilities in applications.

Patching applications and operating systems

3.11 To protect ICT systems from known vulnerabilities, the Top Four mitigation strategies require entities to deploy security patches as soon as possible after being identified by vendors, independent third parties, system managers or users. The timeframe in which patches must be implemented is according to their assessed level of risk. Under the Information Security Manual, patching (or where not available, other mitigating controls) is mandatory within 48 hours of the detection of security vulnerabilities with an extreme risk.

3.12 All three entities have patch management standards that cover the patching of vulnerabilities and help ensure the integrity and authenticity of patches. All three entities conduct checks for vulnerabilities and have developed approaches to address vulnerabilities when defined patches are not available.

32 As discussed in paragraph 1.22, Australia Post's retail environment was not within the scope of this ANAO audit.

3.13 All three entities did not always meet the required timeframes for patching applications and operating systems, including for some extreme risk patches in ASC and Australia Post, and for some non-extreme risk patches within the Reserve Bank.³³ ASC undertook immediate remediation for some of the critical patches for extreme risks that were identified during the audit, and was aware of the challenge in meeting patching requirements within the required timeframes.

3.14 All three entities schedule patching of their applications, and operating systems, using a risk-based approach. When patches were not applied within the required timeframes for applications or operating systems, ASC and the Reserve Bank had other protections in place that were in line with the Top Four mitigation strategies. These were application whitelisting, logging of activities and monitoring. ASC and the Reserve Bank are updating their processes to take into consideration the length of time that patches were not applied and the potential for increased exposure to ICT risks during that time.

3.15 Australia Post remediates patches to desktops and servers, however, patch remediation only occurs for extreme and high risk patches in server environments. This has resulted in remediation activities not occurring within the timeframes required by the entity and under the Information Security Manual. Australia Post operates a number of older operating systems, which has contributed to the patch management challenges. Australia Post is aware of the issues with its patch management and has projects in place to address them and uplift older systems to new versions. These projects are scheduled to be rolled out over the next six months. In the interim, Australia Post advised the ANAO that it has implemented monitoring and other controls to mitigate the risks with its remediation of patches; however, the ANAO's testing of these other controls found that they were generally not sufficient to address the associated risks.

Restricting administrative privileges

3.16 Misuse of privileged access can lead to significant security compromises, such as the unauthorised disclosure of information, systems or processes becoming unavailable, or financial impropriety. The Top Four mitigation strategies include a requirement for administrative privileges to be regularly reviewed, and restricted only to users who need them and are duly authorised.

3.17 All three entities have security policies, standards and guidelines for granting and revoking account access to entity systems and required appropriate authorisation for access to privileged accounts. ASC and the Reserve Bank also have controls in place to prevent users from accessing the Internet from privileged accounts, which would allow sensitive information to be sent to an external site beyond the entity's secure ICT environment; and assigned privileged accounts to administrative groups, not individual accounts. Australia Post allows privileged accounts to access the Internet, but to only an authorised list of websites.

3.18 The Reserve Bank performed quarterly reviews to ensure that users' access to privileged accounts is authorised correctly and monthly assessments of the strength of users' passwords, for example, to ensure that separate passwords are being used for standard access and privileged access accounts. ASC performed monthly revalidation of privileged access and Australia Post performed quarterly user access reviews for some applications and infrastructure. ASC and Australia Post did not perform regular assessments of passwords being used across its network. ASC

33 The Reserve Bank has a policy of applying patches to non-extreme vulnerabilities (high risks and below) within 60 days. This timeframe has not always been met.

had established mitigating controls for this password-related risk that it had assessed to be low and had accepted the implications.

3.19 The Reserve Bank and ASC have enabled logging for their servers and desktops. Australia Post has enabled its servers to log the information required under the Information Security Manual, however, logging has not been configured for Australia Post’s desktops.

Have entities implemented controls that would be in line with the four non-mandatory strategies in the Essential Eight?

ASC and the Reserve Bank have implemented controls in line with all four non-mandatory mitigation strategies in the Essential Eight. Australia Post has implemented controls for one of those mitigation strategies — daily backups of data. All three entities have implemented mitigation strategies beyond the requirements of the Essential Eight, such as the Reserve Bank using machine learning and analytics to detect cyber threats.

3.20 As discussed in paragraph 3.1, in addition to the Information Security Manual’s Top Four mandatory mitigation strategies, an additional four non-mandatory mitigation strategies form a baseline known as the Essential Eight. Table 3.3 describes the four non-mandatory strategies.

Table 3.3: Four non-mandatory mitigation strategies of the Essential Eight

Mitigation strategy	Why apply the strategy?
To prevent malware delivery and execution	
Configure Microsoft Office macro ^a settings	Microsoft Office macros can be used to deliver and execute malicious code on systems.
User application hardening ^b	Flash, Internet advertisements and Java are popular ways to deliver and execute malicious code on systems.
To limit the extent of cyber security incidents	
Multi-factor authentication	Stronger user authentication makes it harder for adversaries to access sensitive information and systems.
To recover data and system availability	
Daily backups	To ensure information can be accessed following a cyber security incident, such as a ransomware incident.




























Note a: Macros are embedded code that can contain a series of commands to automate repetitive tasks.

Note b: Application hardening involves: configuring web browsers to block or uninstall Flash, advertisements and Java on the Internet; and disabling unneeded features in Microsoft Office, web browsers and PDF viewers.

Source: Adapted from Australian Cyber Security Centre documents.

3.21 As shown in Table 3.4, ASC and the Reserve Bank have implemented the four non-mandatory strategies in the Essential Eight. Australia Post has implemented one of the non-mandatory strategies. As with Table 3.2, the results were based on the application of a standard set of assessment criteria and were aggregated to an overall score, which is discussed in more detail in Appendix 3.

Table 3.4: Entities' compliance with the non-mandatory mitigation strategies in the Essential Eight

Control areas assessed	Assessment results								
	Australia Post	ASC	Reserve Bank						
Configure Microsoft Office macro settings									
User application hardening									
Multi-factor authentication									
Daily backups									
<p>Key:</p> <table border="0"> <tr> <td> Controls not in place and no dispensation authorised by the Accountable Authority.</td> <td> Controls in place and meeting control objectives.</td> </tr> <tr> <td> Controls not in place but a dispensation is authorised by the Accountable Authority.</td> <td> Controls in place and maintenance is part of business processes, including monitoring and taking corrective action as required.</td> </tr> <tr> <td> Controls not in place but entity is actively implementing, with a minimum of design deliverables in evidence.</td> <td></td> </tr> </table>				 Controls not in place and no dispensation authorised by the Accountable Authority.	 Controls in place and meeting control objectives.	 Controls not in place but a dispensation is authorised by the Accountable Authority.	 Controls in place and maintenance is part of business processes, including monitoring and taking corrective action as required.	 Controls not in place but entity is actively implementing, with a minimum of design deliverables in evidence.	
 Controls not in place and no dispensation authorised by the Accountable Authority.	 Controls in place and meeting control objectives.								
 Controls not in place but a dispensation is authorised by the Accountable Authority.	 Controls in place and maintenance is part of business processes, including monitoring and taking corrective action as required.								
 Controls not in place but entity is actively implementing, with a minimum of design deliverables in evidence.									

Source: ANAO analysis.

Configure Microsoft Office macro settings

3.22 Effectively configured Microsoft Office macro settings address adversaries' attempts to create macros that can deny users' access to sensitive or classified information. Microsoft Office macro settings should only allow trusted macros in the entity's ICT environment and restrict general and low-privileged users' ability to change macro security settings. The Information Security Manual recommends that entities block all macros in documents taken from the Internet.

3.23 ASC and the Reserve Bank have implemented full controls of Microsoft Office macros. Users are not able to override configured macro settings and can only manage their macros within 'trusted locations'. Both ASC and the Reserve Bank have considered risks associated with users managing their own macros and implemented additional controls that alert their ICT security teams to any potential issues.

3.24 Australia Post's controls do not restrict users' ability to override configured macro settings, including adding and modifying trusted locations. Further, Australia Post has not considered the risks associated with users managing their own macros. Australia Post advised the ANAO that it has configured other controls to mitigate the execution of malicious code. However, the ANAO's testing of these mitigating controls found that not all of the configured controls are applicable to the threats faced, or provide adequate coverage. The ineffectiveness of the other mitigating controls, coupled with the absence of application whitelisting controls, increases Australia Post's risk exposure to malicious code execution. The ANAO notes that Australia Post has included the implementation of appropriate Microsoft Office macro configuration as one of the initiatives in its 'Securing Tomorrow' program.

User application hardening

3.25 When applications are frequently updated and appropriate security settings applied, it is more difficult for adversaries to exploit any security vulnerabilities they may discover. Disabling unneeded features in Microsoft Office and configuring web browsers to block Flash, Internet advertisements and Java further reduces the risk of malicious content being introduced to entities' ICT environments.

3.26 All three entities have standard operating procedures for hardening systems and applications. ASC has a defined standard operating environment to support its ICT environment, which was developed using the Common Operating Environment Policy produced by the Department of Finance. ASC's application hardening security settings are appropriately configured and were implemented in line with its own requirements and the Information Security Manual. The Reserve Bank's standard operating environment was developed using Australian Signals Directorate guidance. Australia Post's standard operating environment was based on Windows and Linux.

3.27 The Reserve Bank blocks Internet advertisements and Flash on web browsers; and has consulted with, and implemented the guidance of, vendors when configuring applications. The Reserve Bank does not block Java content on web browsers, but scans Java files using a malware analysis tool prior to deploying the files to the end-user.

3.28 Australia Post does not block Internet advertisements on its web browsers and Flash or Java on its desktop environments. Australia Post also does not have appropriate security settings applied on Google Chrome or Adobe Reader, such as allowing passwords to be saved and an ability to run outside of protected mode. Australia Post relies on other controls such as security monitoring to detect cyber threats. However, the ANAO's testing found that the other controls in place are insufficient to address the associated risks.

Multi-factor authentication

3.29 Multi-factor authentication requires users to provide at least two independent methods to gain access to an ICT system. These may include:

- something a user knows, such as a password;
- something a user has, such a physical token or software-based certificate; and
- something unique to the user, such as their fingerprint.

3.30 According to the Information Security Manual, entities should use multi-factor authentication for all users; however, certain users such as privileged users, system and database administrators, positions of trust and remote access must use multi-factor authentication. The Information Security Manual also recommends that passwords used in multi-factor authentication processes are not used for other ICT systems.

3.31 ASC and the Reserve Bank have defined requirements for multi-factor authentication and each has implemented multi-factor authentication for privileged users and remote access users. ASC requires multi-factor authentication for users with positions of trust and for general users. The Reserve Bank requires multi-factor authentication for users with access to important data, but not for general users and has instead implemented other controls for general users.

3.32 Australia Post has implemented multi-factor authentication for remote access users, general users and default system accounts, but not for all privileged users. Australia Post relies on monitoring controls to address the risks associated with compromised accounts, however, these controls have not been applied in all environments. Australia Post's 'Securing Tomorrow' program has initiatives to expand the use of multi-factor authentication, including for privileged users.

3.33 ASC and the Reserve Bank both use a combination of a token and a password for multi-factor authentication. ASC and the Reserve Bank use passwords in accordance with the Information Security Manual's standards.

3.34 Australia Post uses a token for remote access users, which meets the Information Security Manual's requirements. Australia Post's documented password standards also meet the requirements of the Information Security Manual, however, the actual implementation does not. Australia Post has completed a risk assessment in regard to this deviation from its security framework.

3.35 All three entities have implemented separate security zones for accessing sensitive ICT assets; ASC and the Reserve Bank require privileged users to re-authenticate by using multi-factor authentication to access the separate security zones. Australia Post requires multi-factor authentication for administrators to access its separate security zones.

Daily backups

3.36 Backups of systems and data are common practices by organisations and support business continuity in the event of disruption to ICT systems, such as through cyber attacks or failures of storage hardware.

3.37 The Information Security Manual recommends that backups:

- of important information are performed daily;
- are stored offline and off-site, or stored online, but configured to be non-rewritable;
- are stored for three months or more; and
- are tested regularly to ensure that information can be restored if the need arises.

3.38 All three entities have documented standard operating procedures for backups, although Australia Post's standards do not detail procedures for performing backups. Australia Post's standards also do not describe its access controls and account management procedures for backups.

3.39 All three entities store their backups both onsite and off-site, and have established processes for restoring backups.

Mitigation strategies beyond the Information Security Manual's Essential Eight

3.40 The Reserve Bank has implemented cyber risk mitigation strategies beyond the requirements of the Information Security Manual's Essential Eight. These strategies focus on enhancing the security functions relating to identification and detection of cyber threats through the use of machine learning and analytics. These strategies can assist with modelling system and user behaviour, and notifying ICT security of potential areas to investigate or focus. ASC is assessing the same capability to support its current security framework.

3.41 Secure coding practices focus on identifying and preventing security flaws during program code development. All three entities have implemented secure coding practices at varying levels. The implementation of these practices is important for entities that develop programs to support their business operations and customers. The practices range from implementing security coding policies and standards to automated penetration testing of software.

4. Cyber security resilience

Areas examined

This chapter examines whether entities are cyber resilient, with a culture of cyber resilience.

Conclusion

The Reserve Bank and ASC are cyber resilient, with high levels of resilience compared to 15 other entities audited over the past five years. Australia Post is not cyber resilient but is internally resilient, which is similar to many of the previously audited entities. The Reserve Bank has a strong cyber resilience culture, ASC is developing this culture, and Australia Post is working towards embedding a cyber resilience culture within its organisation.

Do entities have a cyber resilience culture?

The three entities are at different stages in embedding a cyber resilience culture. The Reserve Bank has a strong cyber resilience culture, having established all 13 assessed behaviours and practices in the areas of cyber security governance and risk management, roles and responsibilities, technical support and monitoring compliance. ASC is developing a cyber resilience culture, having embedded seven of the assessed behaviours and practices and working to more fully establish the other six cyber security behaviours and practices within its business processes. While having embedded eight of the 13 assessed behaviours and practices, Australia Post has not systematically managed cyber risks, including not assessing the effectiveness of controls applied outside its specified cyber security risk management framework. Nevertheless, Australia Post is working towards embedding a cyber resilience culture.

4.1 A cyber resilience culture is comprised of the shared organisational attitudes, values and behaviours that characterise how an entity considers cyber risks in its day-to-day activities.³⁴

4.2 An assessment was undertaken for this audit of whether Australia Post, ASC and the Reserve Bank have a culture of cyber resilience. The assessment expands the analysis of management arrangements, and elements of cyber resilience culture published in Auditor-General Report No.37 2015–16 *Cyber Resilience*, Auditor-General Report No.53 2017–18 *Cyber Resilience* and the July 2018 edition of ANAO Audit Insights.³⁵

4.3 In combination, the presence of the following types of behaviours and practices may assist entities to build a strong cyber resilience culture:

- governance and risk management;

34 Borrowing from the hallmarks of a positive risk culture from the Commonwealth Risk Management Framework. Department of Finance, *Commonwealth Risk Management Policy* [Internet], 2014, available from <https://www.finance.gov.au/comcover/risk-management> [accessed 10 April 2019].

35 Auditor-General Report No.37 2015–16 *Cyber Resilience*, pp. 39–41 [Internet], available from https://www.anao.gov.au/sites/default/files/ANAO_Report_2015-2016_37.pdf [accessed 24 April 2019]; Auditor-General Report No.53 2017–18 *Cyber Resilience*, pp. 43–50 [Internet], available from <https://www.anao.gov.au/work/performance-audit/cyber-resilience-2017-18> [accessed 18 March 2019]; Australian National Audit Office, *Insights from reports tabled April to June 2018* [Internet], available from <https://www.anao.gov.au/work/audit-insights/insights-reports-tabled-april-june-2018> [accessed 24 April 2019].

- roles and responsibilities;
- technical support; and
- monitoring compliance.

4.4 The audit collected evidence of the existence of the behaviours and practices from the three entities. A grading scheme was applied to assess an entity’s capability in the areas that contribute to having a strong cyber resilience culture.

Governance and risk management

4.5 Table 4.1 shows the capabilities assessed for the governance and risk management of cyber risks in the three entities.³⁶

Table 4.1: Governance and risk management capability

Behaviours and practices	Australia Post	ASC	Reserve Bank
Establish a business model and ICT governance that incorporates ICT security into strategy, planning and delivery of services. ^a			
Manage cyber risks systematically, including through assessments of the effectiveness of controls and security awareness training. ^a			
Task enterprise-wide governance arrangements to have awareness of cyber vulnerabilities and threats. ^a			
Adopt a risk-based approach to prioritise improvements to cyber security and to ensure higher vulnerabilities are addressed.			
<p>Key:</p> <ul style="list-style-type: none"> Established. Arrangements in place and maintenance is part of business processes including monitoring and taking corrective action as required. Partially or largely established. Some key elements of the arrangements have not been established. Arrangements have not been established. 			

Note a: This information is also presented in Table 2.2.

Source: ANAO analysis.

4.6 In addition to the analysis in Chapter 2, following Table 2.2, all three entities were found to have:

- leadership from the senior executives and Board to prioritise cyber security and invest in the development of cyber security capabilities;
- governance, audit and risk committees that met regularly to review enterprise and operational level risks, which included reviewing vulnerabilities and potential cyber threats; and

³⁶ The first three capabilities in Table 4.1 that were assessed for the governance and risk management of cyber risks in the three entities were also outlined in Table 2.2 of this report — in the section discussing whether the entities have a fit for purpose cyber security risk management framework.

- staff security awareness programs that address cyber security. In ASC and Australia Post, the security training was holistic and extended to raising awareness of cyber security risks outside of the immediate work environment and to clients.

4.7 As indicated in Table 4.1 and discussed previously, Australia Post has not managed cyber risks systematically. It has not implemented baseline controls on all critical assets, and the controls applied have not been sufficient to address cyber security risks, in particular the protection against the execution of malware code. There was limited evidence of risk or impact assessments to support Australia Post's decision to implement the other controls to address cyber security risks.

4.8 To address cyber security risks, it is important that entities' invest sufficiently in people and ICT assets. All three entities have documented investment plans for their current ICT budgets and projects that include cyber security. Table 4.2 shows the cyber security expenditure for each entity relative to the entity's overall spending.

Table 4.2: Entities' operating and ICT cyber security expenses, 2017–18

Entity	Total operating expenses (\$m)	ICT cyber security expenses (\$m)
Australia Post	\$6,757.6	\$22.0
ASC	\$719.3	\$1.9
Reserve Bank	\$588.0	\$7.1

Source: Based on information advised by the entities and their respective 2017–18 annual reports.

4.9 ASC does not currently have in place a long-term commitment to invest in specific cyber security technology or tools. Instead, business cases for new projects are to be considered on an annual basis, within the existing IT governance framework. Not identifying the criticality of data and systems on its unclassified network makes it difficult for ASC to determine priority in undertaking remediation activities. The Reserve Bank manages its ICT security investments as part of routine business planning processes. ICT projects, including for cyber security, are proposed and assessed annually. The Reserve Bank has in place longer-term strategic initiatives that spanned over two years. The limited visibility of vulnerabilities across Australia Post's critical assets impacts its ability to effectively prioritise improvements to cyber security, particularly for more vulnerable applications.

Roles and responsibilities

4.10 Table 4.3 shows the capabilities assessed under roles and responsibilities for managing cyber risks in the three entities.

Table 4.3: Roles and responsibilities

Behaviours and practices	Australia Post	ASC	Reserve Bank
Assign information security roles to relevant staff and communicate the responsibilities. ^a	◆	◆	◆
Develop the capabilities of ICT operational staff to ensure they understand the vulnerabilities and cyber threats to the system. ^a	▲	▲	◆
Ensure management understand their roles and responsibilities to enhance security initiatives for the services for which they are accountable. This includes senior management understanding the need to oversight and challenge strategies and activities aimed at ensuring the entity complies with mandatory security requirements.	◆	◆	◆
Embed security awareness as part of the enterprise culture, including expected behaviours in the event of a cyber incident.	◆	◆	◆
Assign data ownership to key business areas, including the role to classify the data, and grant or revoke access to shared data by other entities.	◆	▲	◆
<p>Key:</p> <p>◆ Established. Arrangements in place and maintenance is part of business processes including monitoring and taking corrective action as required.</p> <p>▲ Partially or largely established. Some key elements of the arrangements have not been established.</p> <p>■ Arrangements have not been established.</p>			

Note a: This information is also presented in Table 2.2.

Source: ANAO analysis.

4.11 In addition to the expected security roles that were present in all three entities, such as a Chief Information Security Officer, the Reserve Bank has a Business Information Security Officer program. The program operates by nominating an ICT security team member as the point of contact for security related information, and in some instances, working within business teams. The role requires the person to provide suggestions and feedback to the ICT security team, based on their understanding of both the Reserve Bank’s business and security environments.

4.12 In the systems examined, ASC had not clearly assigned the ownership of data to key areas of business. Therefore, the Chief Information Security Officer and Chief Technology Officer (the same person) has responsibility for the operation of the systems and the security and availability of the data held in the systems. The ICT security and operational teams advised the ANAO that they do discuss vulnerabilities, however, these are not formally documented.

4.13 Australia Post has implemented processes to identify vulnerabilities, including threat and risk assessments for projects, and the Information Security Officer provides regular vulnerability reports to operational ICT teams. However, there is limited visibility of threats and risks across the two critical systems examined in this audit — Corporate Data Warehouse and eParcel applications — and detailed security risk assessments for the two critical systems had not been undertaken in the last two years. Internal reviews undertaken by Australia Post also found that security risk assessments had not been performed for its critical systems. Conducting such assessments would increase the awareness of Australia Post’s ICT security and operational staff of the potential

vulnerabilities in critical applications, the level of protection required and current compliance with the entity's baseline controls.

Technical support

4.14 Table 4.4 shows the assessed capabilities for technical support for managing cyber risks in the three entities.

Table 4.4: Technical support

Behaviours and practices	Australia Post	ASC	Reserve Bank
Develop and implement an integrated and documented architecture for data, systems and security controls. ^a	▲	▲	◆
Identify and analyse security risks to their information and system, including documenting ICT assets requiring protection.	▲	▲	◆
Establish a Cyber Incident Response Plan, informed by a comprehensive risk assessment and business continuity plan, including a priority list of services (not ICT systems) to be recovered.	◆	◆	◆
<p>Key:</p> <p>◆ Established. Arrangements in place and maintenance is part of business processes including monitoring and taking corrective action as required.</p> <p>▲ Partially or largely established. Some key elements of the arrangements have not been established.</p> <p>■ Arrangements have not been established.</p>			

Note a: This information is also presented in Table 2.2.

Source: ANAO analysis.

4.15 ASC has defined its unclassified network as a critical asset but has not identified the criticality of data and systems within that network. ASC has documented a standard security baseline and controls within its system security plans, however, could further develop its architecture by defining and documenting the critical assets within the unclassified network and their associated controls. Australia Post has defined a standard security baseline and has defined its critical assets that require protection. Australia Post is yet to complete implementation of all its baseline controls across all its critical assets, and has not performed detailed risk assessments across all critical assets to confirm the required protection and controls.

4.16 As shown in Table 4.4, all three entities have established a cyber incident response plan that lists priority services that are to be recovered as soon as possible in each entity following a cyber security event.

Monitoring compliance

4.17 Table 4.5 shows the assessed capability in all three entities for monitoring compliance with cyber security requirements.

Table 4.5: Monitoring compliance

Behaviours and practices	Australia Post	ASC	Reserve Bank
Develop an approach to verify the accuracy of self-assessments of compliance with cyber security requirements.	◆	◆	◆
<p>Key:</p> <ul style="list-style-type: none"> ◆ Established. Arrangements in place and maintenance is part of business processes including monitoring and taking corrective action as required. ▲ Partially or largely established. Some key elements of the arrangements have not been established. ■ Arrangements have not been established. 			

Source: ANAO analysis.

4.18 All three entities engage external parties to provide support and validate the accuracy of internal reports on the effectiveness of entity ICT controls. For example, the three entities commission assessments under the Information Security Registered Assessors Program from qualified and external ICT professionals.³⁷ Australia Post only performs these assessments for some of its systems as part of contractual requirements with non-corporate Commonwealth entities. Australia Post had also undertaken internal reviews to assess the effectiveness of its cyber security framework, including its self-assessment methodology. These reviews have had observations and findings similar to those in this audit, including that Australia Post has partially implemented its cyber security framework and has not completed detailed risk assessments of critical applications. The findings from these reviews have been incorporated into Australia Post’s initiatives for its ‘Securing Tomorrow’ program.

Are entities cyber resilient?

The Reserve Bank and ASC are cyber resilient as they have met the requirements of their fit for purpose cyber security risk management frameworks. Australia Post is not cyber resilient as it has not met the requirements of its own framework. The Reserve Bank and ASC are also cyber resilient under the requirements of the Information Security Manual, as they have implemented the Top Four cyber security risk mitigation strategies and have effective ICT general controls for logical access and change management. Accordingly, the two entities have a high level of protection from internal and external cyber security threats. Australia Post is not cyber resilient under the requirements of the Information Security Manual, but is internally resilient with effective ICT general controls in place for managing logical access and change processes.

4.19 Cyber resilience refers to entities’ ability to successfully manage cyber intrusions while still delivering core services and business outcomes. Cyber resilience also reduces the likelihood of cyber

³⁷ The Information Security Registered Assessors Program is an initiative to provide high-quality ICT security assessment services to government. Australian Signals Directorate, *Information Security Registered Assessors Program* [Internet], ASD, Australia, 2019, available from <https://acsc.gov.au/infosec/irap/about.htm> [accessed 19 March 2019].

intrusions that threaten Australians' privacy and Australia's social, economic and national security interests.³⁸

4.20 Chapter 2 of this report concluded that Australia Post, ASC and the Reserve Bank all had fit for purpose cyber security risk management frameworks, and that ASC and the Reserve Bank met the requirements of their respective frameworks. On this basis, ASC and the Reserve Bank are cyber resilient. Australia Post has not implemented all the key ICT controls specified in its cyber security risk management framework or put in place effective alternative mitigating controls, and has rated cyber security risk as significantly above its defined tolerance level. On this basis, Australia Post is not cyber resilient.

Cyber resilience under the Information Security Manual

4.21 To enable comparisons with previous ANAO audits of cyber security of non-corporate Commonwealth entities, this chapter examines whether the three entities would be assessed as cyber resilient under the Information Security Manual, by implementing controls in line with the Top Four cyber risk mitigation strategies³⁹ and having effective ICT general controls. Chapter 3 concluded that the Reserve Bank and ASC had implemented the Top Four strategies but Australia Post had not.

ICT general controls

4.22 An entity's ICT general controls are the entity-wide policies, procedures and activities that should be applied to ensure the confidentiality, integrity and availability of ICT systems and data. Effective ICT general controls protect entities from cyber security threats. The controls include:

- logical access management controls for:
 - applications;
 - databases; and
 - operating systems; and
- controls for change management processes.

4.23 Table 4.6 presents the assessment made of the three entities' ICT general controls.

38 Australian National Audit Office, *Insights from reports tabled April to June 2018*, [Internet], available from <https://www.anao.gov.au/work/audit-insights/insights-reports-tabled-april-june-2018> [accessed 8 April 2019].

39 Noting again that as government business enterprises or corporate Commonwealth entities it is not mandatory for the three entities to implement the Top Four strategies in order to meet the requirements of the Information Security Manual, although it is necessary to satisfy the requirements of their own cyber security risk management framework.

Table 4.6: Entities' ICT general controls

Control areas assessed	Australia Post	ASC	Reserve Bank
Logical access management: applications	▲	▲	◆
Logical access management: databases	◆	◆	◆
Logical access management: operating systems	◆	◆	◆
Change management process	◆	◆	◆
<p>Key:</p> <p>◆ Control objective is met.</p> <p>▲ Identified controls not in place, but compensating controls in place and observed.</p> <p>■ Control objective not met.</p>			

Source: ANAO analysis of entity's ICT general controls.

4.24 Table 4.6 shows that only the Reserve Bank had all the expected ICT general controls in place and operating effectively.

4.25 The logical access controls in all three entities were used to:

- grant and revoke user access to applications and control access to databases;
- monitor access to high risk areas and activities for applications and databases; and
- manage security requirements.

4.26 In Australia Post, the monitoring of access to desktop computers and the password requirements for accessing systems in the entity could be improved. In ASC, the logs of user activities did not record the required level of information and were not actively reviewed.

4.27 ICT change management processes in all three entities were documented and supported to:

- record requests for changes to ICT operations, including infrastructure changes;
- authorise changes to systems, programs and data, and manage any impacts on other systems or processes; and
- categorise changes as 'normal', 'standard' or 'emergency'.

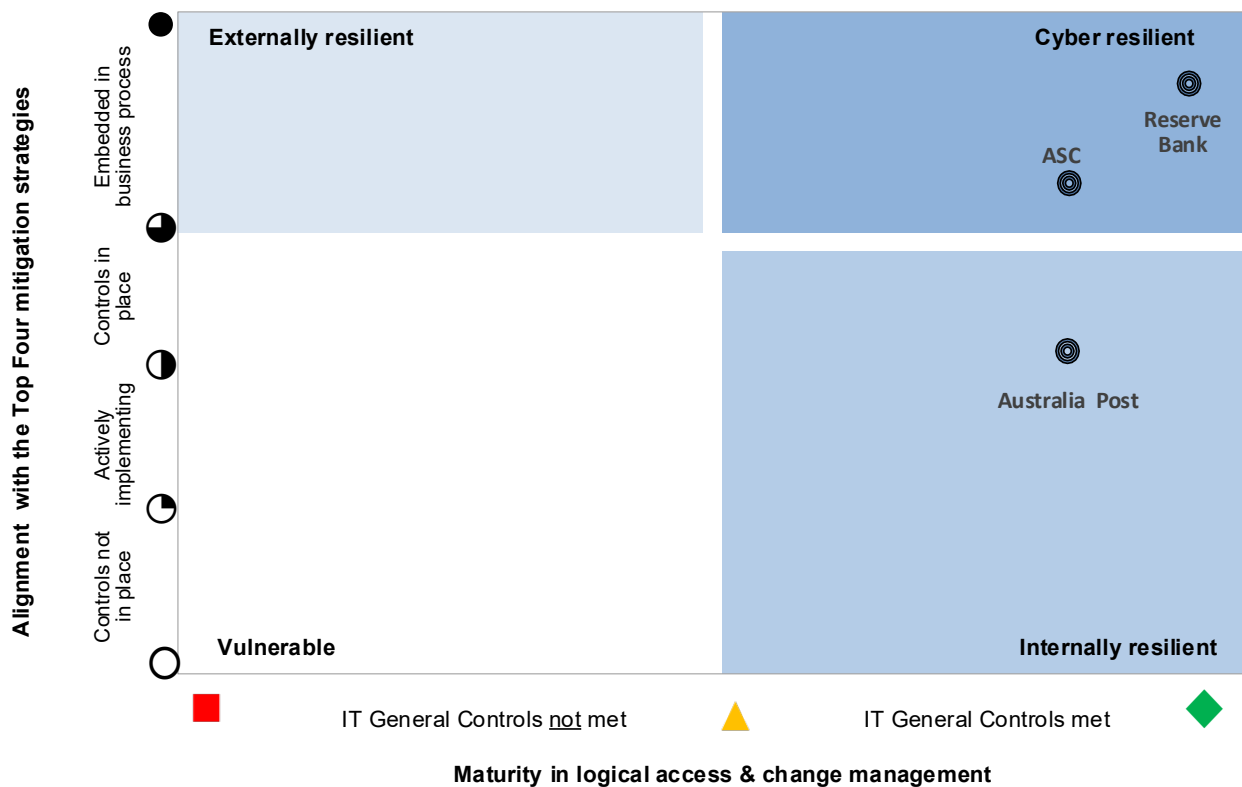
4.28 Australia Post and ASC managed normal and emergency changes as part of their usual change management processes and also had processes for managing changes made out of hours.

4.29 The Reserve Bank had a separate process for managing emergency ICT system changes. The controls in place to manage emergency changes were satisfactory.

Entities' ICT cyber resilience

4.30 In Figure 4.1, the entity's position in the matrix indicates its cyber resilience; that is, how well the entity is protecting its exposure to external vulnerabilities and intrusions, internal breaches and disclosures, and how well it is positioned to address threats. Appendix 3 explains the entity cyber security posture matrix in more detail.

Figure 4.1: Entities’ cyber security resilience



Source: ANAO analysis.

4.31 ASC and the Reserve Bank are in the ‘Cyber Resilient’ zone of the matrix, which means the entities are well placed to address cyber security threats.

4.32 Australia Post is in the ‘Internally Resilient’ zone, which means that it has an adequate level of protection from breaches and disclosures of information from internal sources, but remains vulnerable to intrusions from external sources. While Australia Post has designed its baseline controls in line with the requirements of the Top Four mitigation strategies, it has chosen not to implement these controls across critical applications and instead opted for other controls to address cyber security risks. These other controls have not been sufficient to address cyber security risks.

Australia’s Cyber Security Strategy

4.33 The audit considered the cyber security activities undertaken by Australia Post, ASC and the Reserve Bank that also support the themes in *Australia’s Cyber Security Strategy*. The findings are reported in Appendix 4.

How do entities' cyber security arrangements compare to those of non-corporate Commonwealth entities?

The Reserve Bank and ASC respectively had the highest and equal third highest level of cyber resilience of 17 entities examined by the ANAO over the past five years. Australia Post was not cyber resilient, which was similar to many of the previously audited entities. The small number of government business enterprises and corporate Commonwealth entities assessed (three) means it is not possible to draw conclusions as to the relative level of cyber resilience of corporate compared to non-corporate Commonwealth entities.

4.34 Over the past four years of conducting performance audits of entities' cyber security, the Auditor-General found that only four of 14 non-corporate Commonwealth entities⁴⁰ were cyber resilient.⁴¹

4.35 Figure 4.2 presents the assessments of cyber resilience for all 17 entities audited over the past five years. The assessment of cyber resilience comprised:

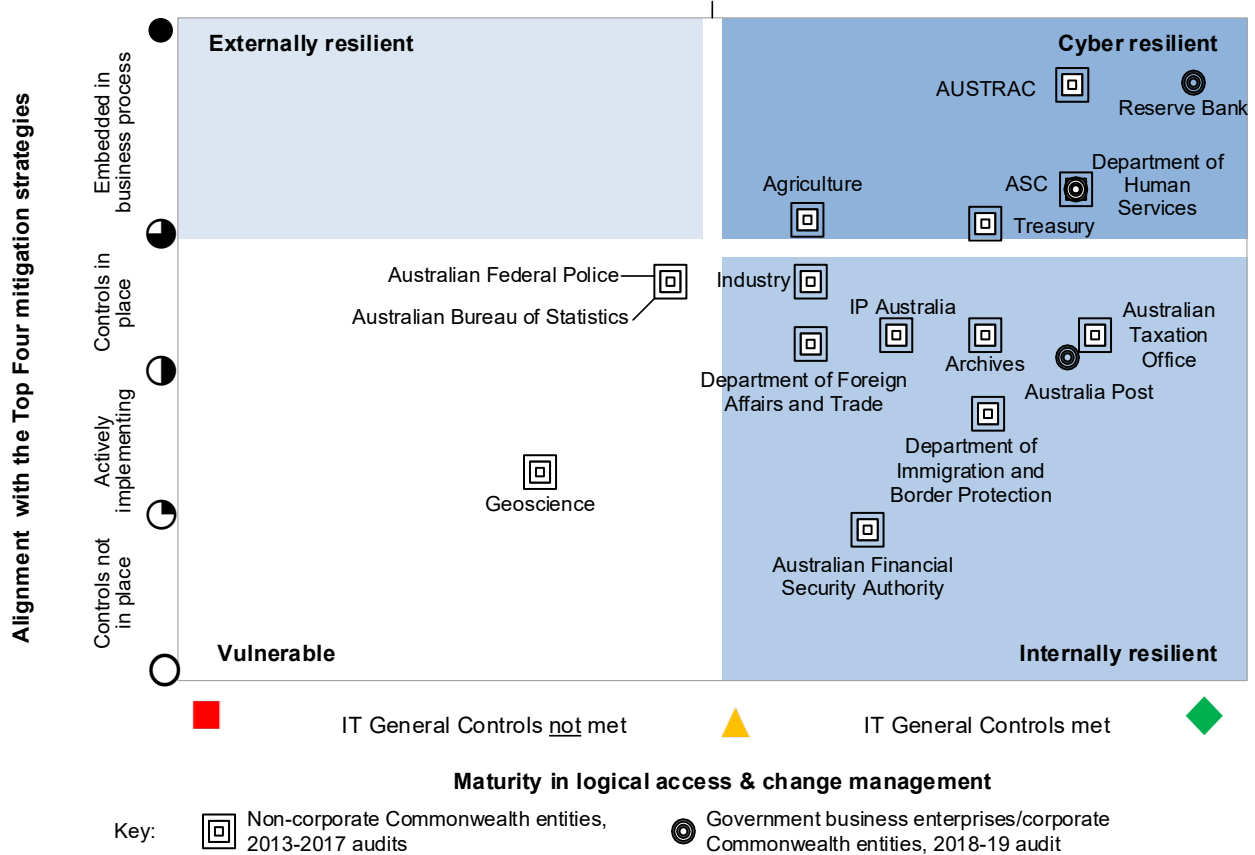
- mandatory compliance with the Top Four mitigation strategies and effective implementation of ICT general controls for 14 non-corporate Commonwealth entities; and
- alignment with the Top Four mitigation strategies and effective implementation of ICT general controls for the three entities selected for this audit.

4.36 The position of each entity in the diagram is the position that was allocated at the time of the latest audit assessment. Apart from Australia Post, ASC and the Reserve Bank, the diagram does not represent the cyber resilience of any other entity in 2018–19.

40 The 14 non-corporate Commonwealth entities examined in those audits held information across the spectrum of economic, commercial, policy and regulatory, national security, program and service delivery and corporate activities. As discussed in Chapter 1, the three entities selected for this audit hold similarly important information and are either a government business enterprise (Australia Post and ASC) or a corporate Commonwealth entity (the Reserve Bank).

41 In particular, there were low levels of compliance for whitelisting, variable levels of compliance for security patching of applications and operating systems (lower for operating systems) and while privileged accounts had some controls, there were also shortcomings in a number of entities.

Figure 4.2: Comparison of entities' cyber resilience



Note: The results on the diagram for the Australian Taxation Office, Department of Human Services and Department of Immigration and Border Protection were from an ANAO follow-up audit and not from the initial audit assessment. The follow-up audit was Auditor-General Report No.42 2016–17 *Cybersecurity Follow-up Audit*.

Source: ANAO analysis.

4.37 Figure 4.2 shows that the Reserve Bank and ASC respectively had the highest and equal third highest level of cyber resilience of all 17 audited entities (government business enterprises, corporate and non-corporate Commonwealth entities). Australia Post was not cyber resilient but was internally resilient, which was similar to many of the previously audited entities.⁴²

4.38 The small number of government business enterprises and corporate Commonwealth entities assessed (three) means it is not possible to draw conclusions as to the relative level of cyber resilience of these entities compared to non-corporate Commonwealth entities.

Grant Hehir
Auditor-General

Canberra ACT
4 July 2019

42 ASC, Australia Post and just under half of the previously assessed non-corporate Commonwealth entities required improvements with the management of logical access to their applications. These were predominantly in the area of user access monitoring. Similar to those non-corporate Commonwealth entities, Australia Post had not implemented application whitelisting. All three entities faced similar challenges in patch management as those of non-corporate Commonwealth entities.

Appendices

Appendix 1 Entity responses

Australian Postal Corporation



17 June 2019

Mr Grant Hehir
Auditor General
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Dear Mr Hehir

Proposed Report on Cyber Resilience – Letter of Reply

Thank you for providing Australia Post the opportunity to provide comment on the proposed report *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities* (Report).

As a government business enterprise operating in a number of competitive markets (including parcel services, government services, financial services, identity services and retail services), Australia Post conducts its complex business operations in a highly competitive commercial environment, maintaining both community and commercial obligations. We provide high-quality, efficient services to the community, and operate commercially to achieve a reasonable return on our assets. In an environment where letters represent a reducing component of our revenue, we seek to expand our range of products and services to meet our commercial objectives. As existing products and services are developed and new products and services introduced, we are committed to upholding the security and integrity of the assets and information we maintain.

Australia Post agrees with Recommendation no. 1. Australia Post has clear oversight of its critical asset infrastructures and has prioritised actions under a program of work already underway to address this recommendation. This will involve conducting risk assessments for critical assets not yet assessed, updating assessments for those already assessed, and taking immediate action to address any concerns that are identified. Monitoring of the implementation of this program of work will be managed through our information security risk management and compliance programs, and will be reported to senior management and our Board, through its Audit & Risk Committee.

Australia Post notes that it has been assessed as 'Internally Resilient' under the grading scheme developed by the Australian National Audit Office and applied in the Report. In our view that determination reflects the significant volume of resources and effort Australia Post has already committed to developing its cyber resilience, but that there is still work to be done to move towards, and maintain, a high level of external resilience.

Australia Post maintains a high level of cyber resilience across its critical platforms and systems supporting government, identity and financial services – a number of which have received external accreditation against the *Australian Government Information Security Manual* (Manual).

Australia Post
111 Bourke Street Melbourne VIC 3000
GPO Box 1777 Melbourne VIC 3000
T: +61 3 9106 7139
M: +61 409 102 122
W: auspost.com.au

Australia Post is not required to apply or comply with the Manual or its Top Four mitigation strategies, but has voluntarily chosen to incorporate aspects of the Manual into its cyber security framework – together with other industry-leading frameworks such as the *National Institute of Standards and Technology Cybersecurity Framework* – as a matter of best practice.

Australia Post is committed to ensuring the security and integrity of its information systems, and to deterring and responding to cyber intrusions. Our continued vigilant focus on the further implementation of our cyber security risk management framework, and on protecting the integrity and security of our systems, will assist in the preservation of a strong framework of cyber resilience for the benefit of our employees, customers and the Australian community.

I acknowledge the work of the Australian National Audit Office and thank you and your staff for providing independent insights set out in the Report, which are of significant importance and value and will contribute to the continuous improvement of Australia Post's cyber resilience.

Thank you again for the opportunity to provide comment on the proposed report.

Yours sincerely,



Christine Holgate
Group Chief Executive Officer and Managing Director



ASC Pty Ltd
ABN 64 008 505 034
GPO Box 2472, Adelaide
South Australia 5001

ASC North
694 Mersey Road North, Osborne
South Australia 5017
T + 61 8 8348 7000
F + 61 8 8348 7001

ASC South
640 Mersey Road North, Osborne
South Australia 5017
T + 61 8 7423 4000
F + 61 8 7423 4090
www.asc.com.au

REF: OUT 000468/2019

4 June 2019

Mr Grant Hehir
Auditor-General for Australia
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Dear Mr Hehir

Re: ANAO proposed audit report on Cyber Resilience of Government Business Enterprises (GBEs) and Corporate Commonwealth Entities.

Thank you for the opportunity to review and provide comment on the proposed audit report on Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities.

ASC agrees with the findings in the report with regard to ASC and is pleased with the ANAO determination that ASC is cyber resilient. ASC will use the detail contained in the report to further strengthen those areas where opportunities to improve have been highlighted by the ANAO audit team.

I would like to express our appreciation of the manner in which the ANAO audit team conducted the audit with the audit activities providing ASC with a thorough and independent review and assessment of our cyber security implementation and posture. ASC believes that both parties exited from the audit with new learnings that will assist us both in future activities around cyber security.

Yours sincerely

Bruce Carter
Chairman

Reserve Bank of Australia



RESERVE BANK OF AUSTRALIA

65 Martin Place
Sydney NSW 2000

GPO Box 3947
Sydney NSW 2001

Philip Lowe
GOVERNOR

+61 2 9551 9507
lowep@rba.gov.au

22 May 2019

Mr Grant Hehir
Auditor-General for Australia
Australian National Audit Office
19 National Circuit
BARTON ACT 2600

Dear Mr Hehir

Thank you for the opportunity to provide comments on the draft report from the Australian National Audit Office's performance audit of cyber resilience.

The Reserve Bank of Australia (RBA) agrees with the findings in the report and that the report is an accurate assessment of our cyber resilience.

The RBA will continue to align with the security controls outlined in the Australian Government Information Security Manual and relevant industry security standards as part of our efforts to maintain a strong financial system for all Australians. The RBA is committed to ensuring that we are a cyber-resilient organisation and we will continue to adapt our security strategy to the changing cyber landscape.

I would like to express my appreciation for the professional and skilled approach taken by your audit team and look forward to further opportunities to support Australia's cyber resilience.

Yours sincerely

A handwritten signature in blue ink that reads "Philip Lowe".

Appendix 2 Recommendations and implementation status from Joint Committee of Public Accounts and Audit Report 467: Cybersecurity Compliance (2017)

Recommendation	Implementation status (April 2019)	Comment
1. The Committee recommends that the Australian Taxation Office (ATO) and Department of Immigration and Border Protection (DIBP) report back to the Committee on their progress to achieving full compliance with the Top Four mitigation strategies by June 2018, including advice as to barriers and timelines to complete outstanding actions.	Implemented ATO: implemented on time by June 2018. Department of Home Affairs (Home Affairs) ^a : implemented in April 2019.	ATO and Home Affairs self-assessed their compliance, see 'Government Response' on the Committee's website. ^b ATO assessed as compliant. Home Affairs assessed as compliant with three of the Top Four, with full compliance by June 2020.
2. The Committee recommends that the Australian Government mandate the Australian Signals Directorate's Essential Eight cybersecurity strategies for all <i>Public Governance, Performance and Accountability Act 2013</i> entities, by June 2018.	Partly agreed to the recommendation but not yet implemented Noted and deferred.	The Government will consider mandating the Essential Eight when cyber security maturity has increased across entities. It agreed to pursue options to extend cyber security requirements to corporate Commonwealth entities.
3. The Committee recommends that the Australian Taxation Office and Department of Immigration and Border Protection report back to the Committee on their progress in implementing Australian National Audit Office (ANAO) Recommendation 1, including advice as to barriers and timelines to complete outstanding actions.	Implemented	ATO and Home Affairs self-assessed their progress, see 'Government Response' on the Committee's website. ^b Both entities' responses emphasised strengthened processes for assessing their cyber security capabilities.
4. The Committee recommends that the Auditor-General consider conducting an audit of the effectiveness of the self-assessment and reporting regime under the <i>Protective Security Policy Framework</i> .	Implemented	The Auditor-General agreed to the Committee's recommendation and reported on findings in Auditor-General Report No.53 2017–18 Cyber Resilience . A potential audit of the 'Cyber resilience of non-corporate Commonwealth entities' was included in the Auditor-General's Draft 2019–20 Annual Audit Work Program.

Recommendation	Implementation status (April 2019)	Comment
5. The Committee recommends that the Attorney-General's Department (AGD) and the Australian Signals Directorate (ASD) report annually on the Commonwealth's cybersecurity posture to the Parliament, such as through the Parliamentary Joint Committee on Intelligence and Security.	Agreed but not yet implemented	The Government agreed that AGD, ASD, and Home Affairs will report annually, and it will consider the appropriate conduit to the Parliament.
6. The Committee recommends that in future audits on cybersecurity compliance, the ANAO outline the behaviours and practices it would expect in a cyber resilient entity, and assess against these.	Implemented	The Auditor-General agreed to the Committee's recommendation and reported on findings in Auditor-General Report No.53 2017–18 Cyber Resilience .
7. The Committee recommends that the Australian Taxation Office and Department of Immigration and Border Protection report back to the Committee on their progress in implementing ANAO Recommendation 2, including advice as to barriers and timelines to complete outstanding actions.	Implemented	ATO and Home Affairs self-assessed their progress, see 'Government Response' on the Committee's website. ^b Both entities' responses emphasised strengthened governance arrangements for cyber security.
8. The Committee recommends that by June 2018, the Australian Government make the annual ASD survey mandatory for all <i>Public Governance, Performance and Accountability Act 2013</i> entities to complete.	Partly agreed and implemented	The <i>Protective Security Policy Framework</i> (October 2018) mandates that non-corporate Commonwealth entities complete the annual ASD survey. The Australian Government will pursue options to extend the annual ASD survey to all corporate Commonwealth entities.
9. The Committee recommends the Australian Government make the Internet Gateway Reduction Program mandatory for all <i>Public Governance, Performance and Accountability Act 2013</i> entities.	Agreed but not yet implemented	The Government agreed to mandate a core Internet Gateway Reduction Program requirement. It will provide further detail on how this recommendation will be implemented as part of related cyber security processes.

Recommendation	Implementation status (April 2019)	Comment
<p>10. The Committee recommends that the Digital Transformation Agency (DTA) report back to the Committee on the review of the Internet Gateway Reduction Program, including:</p> <ul style="list-style-type: none"> • a progress report on the review by December 2017; and • outcomes of the review and associated key actions and corresponding timelines by April 2018. 	<p>Partly implemented</p> <p>No progress report was provided.</p> <p>The review was provided but not the key actions and timelines.</p>	<p>The DTA provided the Committee with a copy of the review in April 2019.</p>

Note a: Formerly the Department of Immigration and Border Protection.












Note b: Responses to the recommendations from the Joint Committee of Public Accounts and Audit *Report 467: Cybersecurity Compliance* [Internet], are available from [https://www.aph.gov.au/Parliamentary Business/Committees/Joint/Public Accounts and Audit/CybersecurityCompliance/Government Response](https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/CybersecurityCompliance/Government_Response).

Source: ANAO analysis and advice from the Secretariat, Joint Committee of Public Accounts and Audit.

Appendix 3 Grading schemes

1. To enable consistent assessments to be made across the three entities in this report, a set of assessment criteria and graphical keys were applied. The keys are represented as either a Harvey Ball or a traffic light symbol. The keys are outlined in Table A.1.

Table A.1: Keys to grading scheme for assessing compliance with an entity’s chosen cyber security risk management framework, alignment with the Top Four mitigation strategies and ICT general controls

Grading scheme for entity’s cyber security risk management framework and the Top Four Information Security Manual’s strategies	Grading scheme for ICT general controls
<p> Controls not in place and no dispensation authorised by the Accountable Authority.</p> <p> Controls not in place, but a dispensation is authorised by the Accountable Authority.</p> <p> Controls not in place, but entity is actively implementing, with a minimum of design deliverables in evidence.</p> <p> Controls in place and meeting control objectives.</p> <p> Controls in place and maintenance is part of business processes, including monitoring and taking corrective action as required.</p>	<p> Control objective not met.</p> <p> Identified controls not in place, but compensating controls in place and observed.</p> <p> Control objective is met.</p>
Grading scheme for assessing capability for managing cyber security risks	
<p> Arrangements have not been established.</p> <p> Partially or largely established. Some key elements of the arrangements have not been established.</p> <p> Established. Arrangements in place and maintenance is part of business processes including monitoring and taking corrective action as required.</p>	

Source: Developed by the ANAO.

2. The selected entities were assessed on their:
- compliance with the requirements of their chosen cyber security risk management framework;
 - alignment with the Top Four mitigation strategies and related controls in the Information Security Manual; and
 - maturity to effectively manage logical access and change management as part of normal business processes (ICT general controls).

3. The summary findings for each of the selected entities are reported in a matrix, using the keys shown in Table A.1, which indicate entities' overall level of protection against internal and external threats as a consequence of steps taken to implement their own mitigation strategies and ICT general controls. The matrix has also been used to show entities' alignment with the Top Four mitigation strategies and ICT general controls. The 'Entity's cyber security posture matrix' indicates where entities are positioned in terms of four cyber resilient zones: Vulnerable; Externally Resilient; Internally Resilient; and Cyber Resilient.

4. The zones are explained further in Table A.2 and illustrated in Figure A.1. An entity's position indicates its cyber resilience; that is, how well the entity is protecting its exposure to external vulnerabilities and intrusions, internal breaches and disclosures, and how well it is positioned to address threats.

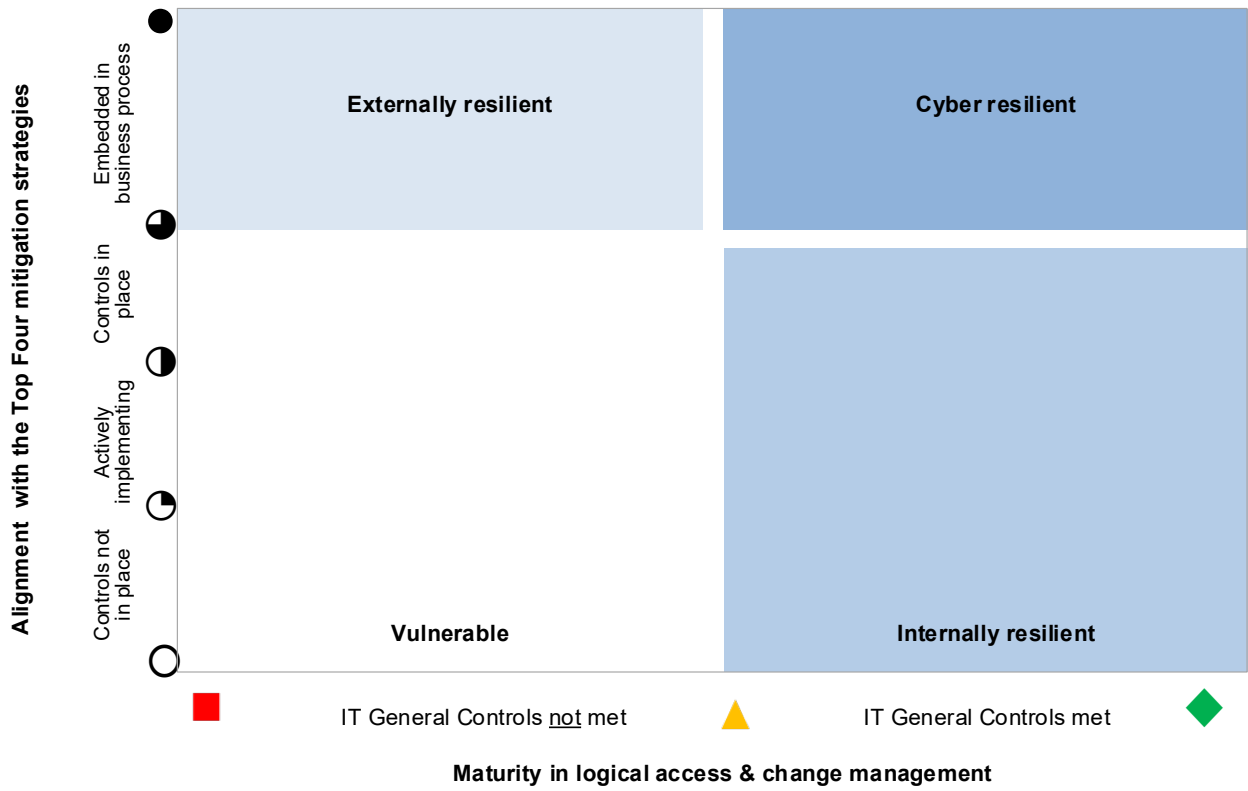
Table A.2: Definitions of the cyber resilient zones

Zone	Definition
Vulnerable	High level of exposure and opportunity for external intrusions and internal breaches and disclosures of information.
Externally Resilient	A level of protection from intrusions from external sources, but vulnerabilities remain to breaches and disclosures from internal sources.
Internally Resilient	A level of protection from breaches and disclosures of information from internal sources, but vulnerabilities remain to intrusions from external sources.
Cyber Resilient	High level of protection from both external intrusions and internal breaches and disclosures of information.

Source: Developed by the ANAO.

5. Figure A.1 shows the matrix used to demonstrate an entity's cyber security risk.

Figure A.1: Entity's cyber security posture matrix



Appendix 4 Australia's Cyber Security Strategy

1. The Australian Government launched *Australia's Cyber Security Strategy* in 2016.⁴³ The strategy set out the Government's philosophy and program for advancing and protecting Australia's interests online.
2. The strategy established five themes of action for Australia's cyber security over the next four years to 2020:
 - a national cyber partnership;
 - strong cyber defences;
 - global responsibility and influence;
 - growth and innovation; and
 - a cyber smart nation.
3. *Australia's Cyber Security Strategy* was reviewed in 2017, about 12 months after its launch. Among the review's findings was that: 'Some of the document's outcomes are not quantifiable, so confidently measuring success is impossible'.⁴⁴ The review's findings and 11 recommendations should be taken into account when considering the contribution of Australia Post, ASC and the Reserve Bank to supporting the five themes in *Australia's Cyber Security Strategy*.
4. ASC is contributing to the development of a national cyber partnership between government, researchers and business. ASC is a member of its local (Adelaide) Joint Cyber Security Centre and attends meetings to increase its awareness of external cyber security issues.⁴⁵
5. All three entities are aware of and addressing the need for stronger cyber defences in government business enterprises and corporate Commonwealth entities that will better detect, deter and respond to threats and anticipate emerging cyber security risks.
6. As Australia's central bank, and having a strong cyber resilience culture, the Reserve Bank shares information, learnings and practices with other organisations both within the financial sector and more broadly to support cyber security. The Reserve Bank's actions support its own operations and contribute to global goals for reducing cybercrime and its impact on government, business and individuals.
7. Similar to the Reserve Bank, Australia Post does share information, learnings and practices with other organisations, however, not as extensively within its own industry. Australia Post has broadened its security awareness program to its customers through its retail presence to help increase awareness of good security practices and current cyber threats amongst its customers.

43 Department of Prime Minister and Cabinet, *Australia's Cyber Security Strategy* [Internet], DPM&C, Australia, 2016, available from <https://www.pmc.gov.au/sites/default/files/publications/australias-cyber-security-strategy.pdf> [accessed 25 February 2019]. The Home Affairs portfolio subsequently assumed responsibility for cyber security policy and coordination.

44 The Australian Strategic Policy Institute, *Australia's Cyber Security Strategy: Execution and Evolution* [Internet], ASPI, Canberra, 2017, p. 3 and pp. 16–17, available from https://i.nextmedia.com.au/Assets/ASPI_cyber_security_strategy_review.pdf [accessed 20 March 2019].

45 Information about the national network of Joint Cyber Security Centres is available from <https://www.cyber.gov.au/about-this-site/about-acsc/> [accessed 20 March 2019].