The Auditor-General
ANAO Report No.53 2017–18
Performance Audit

Cyber Resilience

Department of the Treasury

National Archives of Australia

Geoscience Australia

Australian National Audit Office

ISSN 1036–7632 (Print)
ISSN 2203–0352 (Online)
ISBN 978-1-76033-372-0 (Print)
ISBN 978-1-76033-373-7 (Online)

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

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

Australian National Audit Office

Canberra ACT

28 June 2018

Dear Mr President
Dear Mr Speaker

The Australian National Audit Office has undertaken an independent performance audit in the Department of the Treasury, the National Archives of Australia and Geoscience Australia titled *Cyber Resilience.* The audit was conducted in accordance with the authority contained in the *Auditor-General Act 1997*. 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

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

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

Audit team

Alex Doyle
William Na
Matthew Rigter
Lisa Elkner
Kelvin Le
Carissa Chen
Pooja Bajaj
Elenore Karpfen
Andrew Morris

Contents

Summary and recommendations

Background

1. Cyber security is a strategic priority for the Australian government.[1] A secure cyberspace provides trust and confidence for individuals, business and the public sector to share ideas, collaborate and innovate.[2] To strengthen trust online, effective implementation of a comprehensive cyber security strategy across government systems is critical to protect Australians' privacy and Australia's social, economic and national security interests from targeted cyber intrusions and emerging cyber threats. The Attorney-General's Department *Protective Security Policy Framework* outlines the core requirements for the effective use of protective information and communications technology (ICT) security.

2. In February 2017, the Australian Signals Directorate issued the updated *Strategies to Mitigate Cyber Security Incidents* as a priority list of practical actions entities can take to make their ICT environment more secure. It referred to these cyber security strategies as the Essential Eight and recommended that entities implement the strategies as a security baseline. In June 2017, the Australian Signals Directorate also released the *Essential Eight Maturity Model*, to assist entities to assess the level of implementation of the Essential Eight mitigation strategies. A revised Model was issued in October 2017.

3. Of the eight mitigation strategies, four are mandatory (the Top Four).[3] Since 2013, entities have been required to undertake an annual self-assessment against the mandatory requirements of the *Protective Security Policy Framework*. Key elements to achieving compliance with the mandatory mitigation strategies are: sufficient investment; appropriate processes; and a culture that recognises the importance of and requirements for cyber resilience.

4. Three entities were included in the audit: Department of the Treasury (Treasury), National Archives of Australia (National Archives), and Geoscience Australia. These entities were selected based on the character and sensitivity of the information collected, stored and reported.

5. Since 2013–14, the Australian National Audit Office (ANAO) has conducted three performance audits to assess the cyber resilience of 11 different government entities.[4] These audits have identified high rates of non-compliance with the requirements of the *Protective Security Policy Framework*.

1 Joint Committee of Public Accounts and Audit, *Report 467: Cybersecurity Compliance*, 2017, p. 13, available from <http://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024076/toc_pdf/Report467CybersecurityCompliance.pdf;fileType=application%2Fpdf>, [accessed 9 January 2018].

2 Prime Minister and Cabinet, *Australia's Cyber Security Strategy* [Internet], 2016. Available at <https://cybersecuritystrategy.pmc.gov.au/>, [accessed 9 January 2018].

3 The Top Four strategies are application whitelisting, patching applications, patching operating systems, and minimising privileged user access. The non-mandatory strategies are disabling untrusted Microsoft Office macros, user application hardening, multi-factor authentication, and daily backup of systems and data.

4 ANAO Report No.50 2013–14, *Cyber Attacks: Securing Agencies' ICT System*; ANAO Report No.37 2015–16 *Cyber Resilience*; and ANAO Report No.42 2016–17 *Cybersecurity Follow-up Audit*.

Audit rationale

6. The ANAO decided to conduct this fourth audit of entities' management of cyber risks recognising ongoing parliamentary interest (including enquiries by the Joint Committee of Public Accounts and Audit) and the level of non-compliance with mandatory requirements identified in previous audits. In *Report 467: Cybersecurity Compliance*, the Joint Committee of Public Accounts and Audit recommended that the ANAO outlines the behaviours and practices it would expect in a cyber resilient entity and assess against these.

Audit objective and criteria

7. The objective of the audit was to assess the effectiveness of the management of cyber risks by the Department of the Treasury, National Archives of Australia and Geoscience Australia.

8. The audit criteria were:

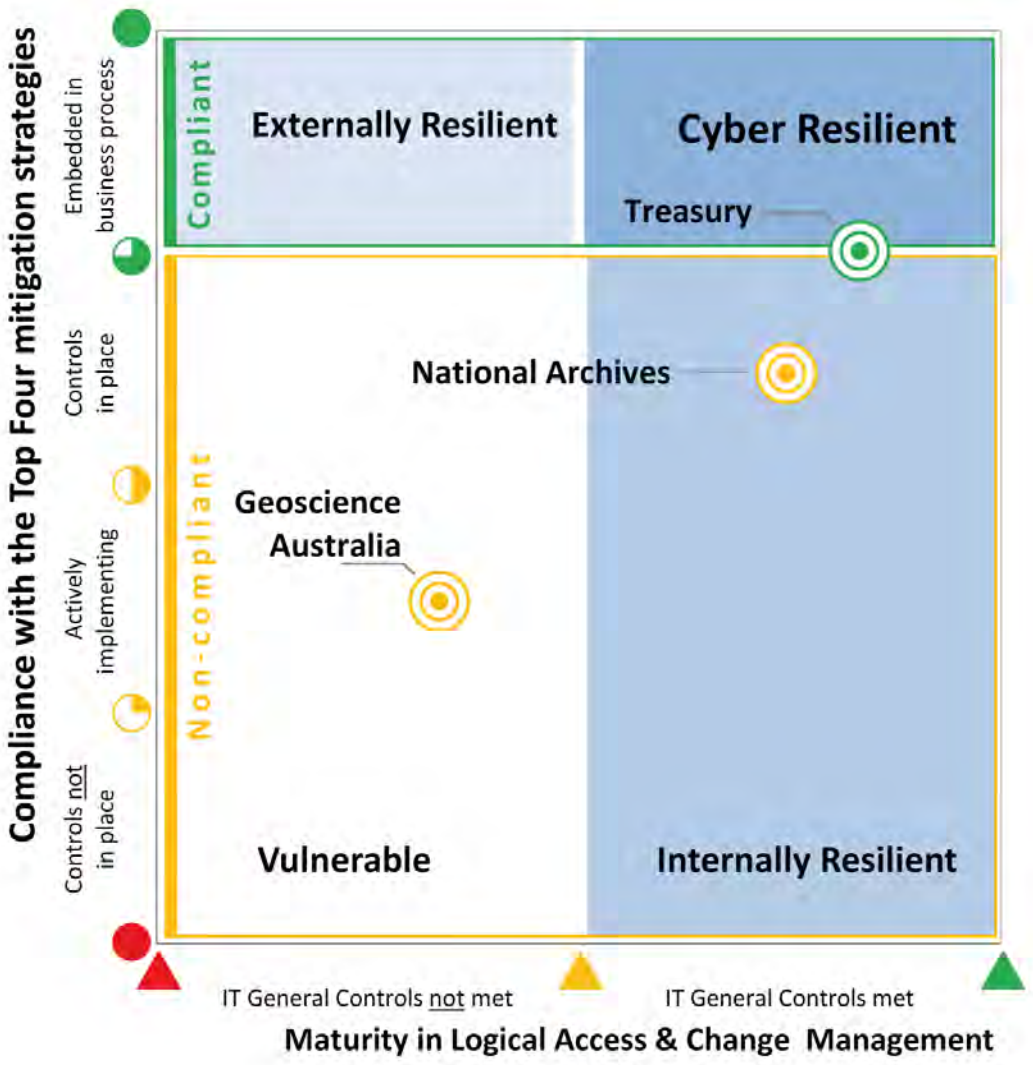
- do entities have effective arrangements in place for managing cyber risks;
- do entities monitor and report against cyber security deliverables; and
- were entities cyber resilient, with a culture of cyber resilience?

Conclusion

9. As with the ANAO's previous audits of cyber security, this audit identified relatively low levels of effectiveness of Commonwealth entities in managing cyber risks, with only one of the three audited entities compliant with the Top Four mitigation strategies. None of the three entities had implemented the four non-mandatory strategies in the Essential Eight and were largely at early stages of consideration and implementation. These findings provide further evidence that the implementation of the current framework is not achieving compliance with cyber security requirements, and needs to be strengthened.

10. Of the three entities, only Treasury was compliant with the Top Four mitigation strategies and cyber resilient. National Archives was not compliant with the Top Four mitigation strategies but had sound ICT general controls and so was assessed as not cyber resilient but internally resilient. Geoscience Australia was not compliant with the Top Four mitigation strategies and did not have sound ICT general controls so was assessed as vulnerable to cyber attacks. All three entities had implemented only one of the four non-mandatory mitigation strategies in the Essential Eight, and were not well progressed in considering an implementation position for the other three strategies. Figure S.1 shows each entity's cyber resilience.

Figure S.1: Entities' cyber resilience[a]



KEY:

- Control ***not*** in place and ***no*** dispensation authorised by the Accountable Authority.
- Control ***not*** in place but a dispensation is authorised by the Accountable Authority.
- Control ***not*** in place but entity is actively implementing, with a minimum of design deliverables in evidence.
- Control in place and meeting control objectives.
- Control in place and maintenance is part of business processes, including monitoring and taking corrective action as required.
- Control objective ***not*** met.
- Identified control ***not*** in place but compensating controls in place and observed.
- Control objective is met.

Note a: An entity's position on the matrix indicates its overall cyber resilience—in essence how well the entity is protected from external intrusions, internal breaches and unauthorised disclosures of information, and how well it is positioned to address threats.

Source: ANAO analysis.

11. Two entities had accurately self-assessed and reported their level of compliance with the Top Four mitigation strategies, and the other entity had not. There are shortcomings in the *Essential Eight Maturity Model* that limits its usefulness in its current form, and could lead to entities inadvertently overstating their cyber security compliance if it is used in performing the self-assessment. With activities underway to revise security reporting under the *Protective Security Policy Framework,* it is timely to also strengthen guidance supporting entities to self-assess compliance with the mandatory mitigation strategies and processes to verify the correctness of those assessments.

12. The three entities had partly effective arrangements for managing cyber security risks, with specialist staff in dedicated security positions contributing to existing ICT processes and broader business models. However, the entities did not adopt a risk-based approach to prioritise improvements to cyber security, with cyber security investments focused on short-term operational needs rather than long-term strategic objectives. Until the National Archives and Geoscience Australia achieve compliance with the mandatory strategies, it is inappropriate to consider that a positive cyber resilience culture is in place.

Supporting findings

Implementation of cyber risk mitigation strategies

13. Treasury complied with the requirements of the Top Four mitigation strategies, while National Archives and Geoscience Australia did not comply. National Archives met the requirements for two of the strategies, patching ICT applications and minimising privileged user access, but not for application whitelisting or patching operating systems. Geoscience Australia was not compliant with any of the four strategies.[5]

14. Of the three entities, only Treasury was cyber resilient, with a high level of protection from external intrusions and internal breaches. The department complied with the Top Four mitigation strategies and had sound ICT general controls in place for logical access and change management. The ANAO assessed National Archives as internally resilient but vulnerable to attacks from external sources. Geoscience Australia was assessed as vulnerable, with a high level of exposure and opportunity for external attacks and internal breaches and unauthorised disclosures of information.

15. The three entities had each implemented one of the four non-mandatory strategies in the Essential Eight—daily backup of important data. Treasury, National Archives and Geoscience Australia had made limited progress in implementing the other three non-mandatory strategies—disabling untrusted Microsoft Office macros, user application hardening and multi-factor authentication. In a few instances, the entities had considered risks and commenced developing plans to implement controls as part of the non-mandatory strategies, but were generally not well progressed in determining an implementation position for the strategies.

5 Geoscience Australia had recently reassessed its cyber security arrangements and commenced an IT program of work to achieve compliance with the Top Four mitigation strategies, including deploying application whitelisting for critical ICT infrastructure, by late 2018.

Self-assessment and maturity model

16. All three entities conducted self-assessments against the Top Four mitigation strategies and reported their compliance in accordance with government requirements. Treasury and Geoscience Australia accurately assessed their level of compliance. National Archives incorrectly reported compliance against two strategies. In conducting the self-assessments, the entities did not have access to comprehensive guidance or supporting tools, such as control assessment test plans or grading schemes, which would have assisted accurate self-assessments according to the requirements of the *Protective Security Policy Framework*.

17. In its current form, the *Essential Eight Maturity Model* is unlikely to achieve its objective of assisting entities to determine their maturity in implementing the Essential Eight mitigation strategies. This is primarily because there is inconsistent and incomplete alignment between the definitions of the mitigation strategies in the *Australian Government Information Security Manual* and the criteria for attaining a particular maturity level in the *Essential Eight Maturity Model* document.

18. A revised *Protective Security Policy Framework* and updated reporting requirements is scheduled for 2018–19. In light of the continued low level of compliance with the Top Four mitigation strategies, the revised framework should incorporate adequate technical guidance to support entities to accurately self-assess against those strategies, additional verification of compliance with those requirements and enhanced transparency about entities' compliance.

Management arrangements and cyber resilience culture

19. The three entities had partly effective arrangements for managing cyber security risks, with scope for improvement in important elements of risk management and governance. Two of the three entities had established a business model and ICT governance that incorporated ICT security into strategy, planning and delivery of services, and all entities had key ICT operational staff with a sound understanding of the vulnerabilities and cyber threats that may affect their ICT systems. The three entities had not adopted a systematic risk-based approach to prioritise improvements to cyber security across their ICT systems, or identified and documented cyber initiatives beyond 2017–18, and key ICT security management roles had not been consistently filled.

20. The three entities were at different stages in embedding a cyber resilience culture. Treasury was aware of the importance of its sensitive data holdings and had ongoing activities to strengthen its cyber security approaches. National Archives had a number of longstanding practices and could have learnt more from looking outwardly to the cyber resilience practices of other entities. Geoscience Australia has traditionally had a culture of scientific independence that it had allowed to override cyber resilience considerations. All entities are aiming to better understand the shared attitudes, values and behaviours to make the most of ICT opportunities while effectively managing cyber risks.

Recommendations

Recommendation no.1
Paragraph 2.15

Geoscience Australia and National Archives of Australia each establish a plan and timeframe to achieve compliance with the Top Four mitigation strategies, and monitor delivery against that plan.

Geoscience Australia response: *Agreed*.

National Archives of Australia response: *Agreed*.

Recommendation no.2
Paragraph 3.39

In revising security reporting and cyber-related requirements under the *Protective Security Policy Framework*, the Attorney-General's Department, Department of Home Affairs and Australian Signals Directorate work together to improve compliance with the framework by:

(a) providing adequate technical guidance to support entities to accurately self-assess compliance with the Top Four mitigation strategies and their underlying controls contained in the Information Security Manual;

(b) developing a program for verifying entities' reported compliance with the mandatory cyber security requirements; and

(c) increasing transparency and accountability about entities' compliance with those requirements.

Attorney-General's Department response: *Agreed to part (a) and part (c); Agreed in principle to part (b).*

Department of Home Affairs response: *Agreed*.

Australian Signals Directorate response: *Agreed*.

Summary of entity responses

21. Entities' responses to the proposed report are provided at Appendix 1 and entities that provided summaries of their responses have been included below.

Department of the Treasury

The Treasury agrees with the findings and the recommendation within the performance audit of Cyber Resilience, dated 16th May 2018. The Information Security Manual will continue to be used to inform future cyber security strategies and policies for the department.

The Treasury acknowledges the importance of diligence and attentiveness to cyber security for all Treasury staff. The Treasury will continue to develop and implement robust cyber security strategies and policies to strengthen the security of ICT systems to mitigate the risk of cyber intrusion.

National Archives of Australia

The National Archives will develop a cyber resilience framework and a supporting plan to effectively implement the Essential Eight. It is intended the framework will underpin a secure, stable and contemporary ICT environment that supports the business of the National Archives. The activities to achieve the cyber maturity model for the National Archives will be prioritised by

the National Archives Enterprise Board taking into consideration resourcing and whole-of-government posture for cyber resilience.

Geoscience Australia

Geoscience Australia welcomes this report and agrees with the two recommendations. We agree that the report is an accurate assessment of our compliance at the time of the audit.

Geoscience Australia is committed to improving its security compliance and cyber resilience to a level appropriate for a government organisation that plays a role in providing scientific information and services to industry and the broader community.

We have already commenced actions to improve compliance to address the security issues identified including: the engagement of a senior consultant to advise on an overarching security framework; the establishment of a Security Working Group; and an action plan to address compliance with the Australian Signals Directorate's *Strategies to mitigate cyber security incidents*.

Key learnings for improvement for all Australian Government entities

22. Below is a summary of behaviours and practices identified in this and previous audit reports that, if implemented, may improve the level of cyber resilience of Commonwealth entities. A more comprehensive list is at Table 4.3 of this report. These learnings include expected, appropriate behaviours and practices of a cyber-resilient entity that the ANAO has observed from audits of cyber security that entities can apply to embed a culture of cyber resilience.[6]

Governance and risk management

- Self-assess the Top Four cyber security risk mitigation strategies of the *Protective Security Policy Framework* using a controls-based approach. If the self-assessment is non-compliance, make the necessary investments and changes to become compliant.
- Make decisions about how and when to implement the four non-mandatory strategies in the Essential Eight mitigation strategies promulgated by the Australian Signals Directorate.
- Establish a business model and ICT governance that incorporates ICT security into strategy, planning and delivery of services.
- 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.
- Manage cyber risks systematically, including through assessments of the effectiveness of controls, security awareness training, and adopting a risk-based approach to prioritise improvements to cyber security.
- Assign information security roles to relevant staff and communicate the responsibilities.

6 The ANAO will continue to refine this list of behaviours and practices in response to Recommendation 6 in the Joint Committee of Public Accounts and Audit's *Report 467: Cybersecurity Compliance.*

Audit findings

1. Background

Introduction

1.1 The Australian Signals Directorate[7] has prioritised a list of security initiatives that Australian Government entities should take to secure their information and communications technology (ICT) systems against cyber intrusions and threats.[8] In April 2013, the Australian Government *Protective Security Policy Framework*[9] mandated that government entities implement the top four of these 37 strategies (Top Four mitigation strategies).[10]

1.2 The Top Four mitigation strategies are:

- using application whitelisting[11] on desktops and servers to prevent malicious software and unapproved programs from running on a computer;
- applying application patches[12] through sound policies, procedures and practices to help ensure the applications' security;
- applying operating system patches through sound policies, procedures and practices to mitigate security risks and reduce system vulnerabilities; and
- effectively managing access provisions for privileged user accounts[13] across an entity's ICT environment, including the entity's network, applications, databases and operating systems.

1.3 In February 2017, the Australian Signals Directorate recommended the inclusion of four additional security strategies to prevent malware running on ICT systems, limit the extent of incidents and recover data. The Australian Signals Directorate updated its cyber security strategies from the Top Four mitigation strategies in response to the increasing threat of ransomware.[14]

7 The Australian Signals Directorate is an intelligence entity in the Department of Defence, and provides information security advice and services to Australian federal and state government entities.

8 According to the Australian Signals Directorate, this guidance is informed by its experience in responding to cyber security incidents and performing vulnerability assessments and penetration testing of Australian government organisations.

9 The Australian Government *Protective Security Policy Framework* is administered by the Attorney-General's Department. It is available from <https://www.protectivesecurity.gov.au/Pages/default.aspx>, [accessed 8 January 2018].

10 As at May 2018, there was no explicit mention of the Top Four mitigation strategies in the *Protective Security Policy Framework*. Instead, the link to the *Protective Security Policy Framework* was through INFOSEC 4, which required entities to 'implement the mandatory *Strategies to Mitigate Targeted Cyber Intrusion* as detailed in the *Australian Government Information Security Manual*.'

11 A whitelist is a list of trusted executables. It is a more practical and secure method of securing a system than proscribing a list of untrusted executables that are to be prevented from running (a blacklist).

12 A patch is a piece of software designed to fix problems with, or update, a computer program or its supporting data. This includes fixing security vulnerabilities.

13 System administrators typically have greater access rights to systems and information than normal users.

14 Ransomware is a type of malicious software designed to block user access to a computer system until a sum of money is paid.

1.4 The additional security strategies are:

- disabling untrusted Microsoft Office macros on desktops and servers to prevent the unauthorised download and running of malicious software;
- hardening the configuration of applications (user application hardening) used to interact with the Internet, including blocking web browser access to Adobe Flash player, web advertisements and untrusted Java code;
- applying multi-factor authentication to make it more difficult for adversaries to use stolen credentials to access sensitive information and facilitate further malicious activities across an entity's ICT environment; and
- effectively managing daily backup of important data, including testing of data restoration processes, to mitigate data being encrypted, corrupted or deleted by ransomware or other destructive malicious software.

1.5 These four strategies complement the Top Four mitigation strategies—and are collectively known as the Essential Eight.[15] The current cyber threat is such that the Australian Signals Directorate recommends that entities implement a package of eight essential mitigation strategies as a security baseline. Only four of the eight strategies—the (original) Top Four—are mandatory.[16]

1.6 To effectively implement the Essential Eight, an entity must have a sound enterprise-wide ICT general controls framework. This framework provides an entity with a stable and reliable ICT environment and forms the foundation upon which other processes and controls can be built. ICT general controls include controls over: ICT governance; ICT infrastructure; acquiring and developing applications; logical user access[17] to ICT infrastructure, applications and data; and making changes to ICT systems and applications.

Self-assessments, previous audits and cyber security culture

1.7 Since 2013, non-corporate Commonwealth entities have been required to undertake an annual self-assessment against the mandatory requirements of the *Protective Security Policy Framework*. Entities are required to annually report their compliance to the relevant portfolio Minister and the Secretary of the Attorney-General's Department and provide a copy to the Auditor-General by August each year. The Top Four mitigation strategies are part of the self-assessment criteria.

1.8 Since 2013–14, the Australian National Audit Office (ANAO) has conducted three performance audits to assess the cyber resilience of 11 different government entities.[18] These audits assessed entities' implementation of the Top Four mitigation strategies and ICT general controls,

15 Australian Signals Directorate, *Essential Eight Maturity Model* [Internet], 2017, available from <https://www.asd.gov.au/publications/protect/essential-eight-maturity-model.htm>, [accessed 8 January 2018]. The Essential Eight are also described in Appendix 3.

16 The Joint Committee of Public Accounts and Audit, in *Report 467: Cybersecurity Compliance,* recommended that the Australian Government mandate the Essential Eight cybersecurity strategies for all *Public Governance, Performance and Accountability Act 2013* entities by June 2018.

17 Logical access controls are tools and protocols used for identification, authentication, authorisation, and accountability in ICT systems.

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

which are required by the *Protective Security Policy Framework*. The ANAO has also reviewed the self-assessment of compliance with the mandatory strategies, as reported by entities.[19]

1.9 In June 2017, the Joint Committee of Public Accounts and Audit (JCPAA) held a public hearing to discuss the findings of the third ANAO audit on cyber security.[20] The JCPAA, in *Report 467: Cybersecurity Compliance* released in October 2017, considered that all non-corporate Commonwealth entities should be compliant with the Top Four mitigation strategies by 30 June 2018. The JCPAA also noted that 'key elements to achieve compliance with the mandatory mitigation strategies are a significant investment, as well as a culture which recognises the importance of, and requirement for cyber resilience.'[21] The JCPAA made 10 recommendations; including two for the ANAO:

- Recommendation 4—The Committee recommends that the Auditor-General consider conducting an audit of the effectiveness of the self-assessment and reporting regime under the *Protective Security Policy Framework*.
- Recommendation 6—The Committee recommends that in future audits on cyber security compliance, the ANAO outline the behaviours and practices it would expect in a cyber resilient entity, and assess against these.[22]

1.10 In relation to Recommendation 4, this audit has addressed, for the three audited entities, the effectiveness of the current self-assessment and reporting regime for the *Protective Security Policy Framework.* The ANAO will consider conducting an audit of the effectiveness of the revised self-assessment and reporting regime (which is planned to be implemented from 2018–19) when developing future annual audit work programs. In respect of Recommendation 6, in this audit the ANAO has drawn on previous audit work[23] to assess the cyber resilience of the three audited entities, and has outlined additional behaviours and practices of cyber resilient entities to assess against in future cyber security audits (reported in Chapter 4).

Audit approach

1.11 The ANAO decided to conduct this fourth audit of entities' management of cyber risks recognising ongoing parliamentary interest (including enquiries by the JCPAA) and the level of non-compliance with mandatory requirements identified in previous audits. In *Report 467: Cybersecurity Compliance*, the JCPAA recommended that the ANAO outlines the behaviours and practices it would expect in a cyber resilient entity and assess against these.

1.12 The three Australian Government entities included in this audit are significant users of technology and were selected based on the character and sensitivity of the information collected, stored and reported:

- the Department of the Treasury analyses economic and fiscal data to advise the Government on effective government spending and taxation arrangements, including

19 The conclusions and findings of these audits are discussed in Chapter 4.
20 ANAO Report No.42 2016–17 *Cybersecurity Follow-up Audit*.
21 JCPAA, *Report 467: Cybersecurity Compliance*, October 2017, p. 3.
22 JCPAA, *Report 467: Cybersecurity Compliance*, October 2017, p. vii and viii.
23 Including ANAO Audit Report No.37, 2015–16, *Cyber Resilience*, p. 41.

trends in Commonwealth revenue and major expenditure programs, and the annual preparation of the Commonwealth Budget;

- National Archives of Australia plays a key role in collecting and preserving Australian Government records that reflect the nation's history and identity; and
- Geoscience Australia applies science and technology to assist government and the community to make informed decisions about the use of natural resources, management of the environment, and community safety. In addition, it provides critical services such as tsunami warnings and monitoring of bushfires, earthquakes and nuclear tests.

Table 1.1 outlines the type of information collected, stored and used by these entities.

Table 1.1: Key information collected, stored and used by the selected entities

Entity	Economic information	Policy and regulatory	National security	Program and service delivery	Personal
Department of the Treasury	✓	✓	✓	N/A	N/A
Geoscience Australia	✓	✓	✓	✓	N/A
National Archives of Australia	✓	✓	✓	✓	✓

Source: ANAO analysis.

1.13 The objective of the audit was to assess the effectiveness of the management of cyber risks by the Department of the Treasury, National Archives of Australia and Geoscience Australia.

1.14 The audit criteria were:

- do entities have effective arrangements in place for managing cyber risks;
- do entities monitor and report against cyber security deliverables; and
- were entities cyber resilient, with a culture of cyber resilience?

1.15 The scope of the audit was to assess whether the selected entities were compliant with the Top Four mitigation strategies mandated in the *Protective Security Policy Framework*, and the extent to which the entities had implemented, or planned to implement, the four non-mandatory mitigation strategies of the Essential Eight. The audit also examined aspects of entities' arrangements for developing a culture of cyber resilience.

1.16 In undertaking the audit, the ANAO:

- assessed the actions taken by the selected entities in prioritising cyber risks through effective ICT governance and risk management frameworks;
- assessed the Essential Eight cyber security strategies and the underlying controls as per the Australian Signals Directorate's Information Security Manual, with an emphasis on the Top Four mandatory mitigation strategies; and
- reviewed the business model and ICT governance, and the cyber resilience culture.[24]

24 The ANAO provided detailed briefings regarding the specific findings of the audit to senior executives, ICT Security Advisors, senior managers and officers of ICT operations within each entity. A detailed technical paper outlining specific findings was also provided to each entity.

1.17 The assessments were made in late 2017 through early 2018.

1.18 The audit was conducted in accordance with the ANAO Auditing Standards at a cost to the ANAO of approximately $440 000.

1.19 Team members for the audit were Alex Doyle, William Na, Matthew Rigter, Lisa Elkner, Kelvin Le, Carissa Chen, Pooja Bajaj, Elenore Karpfen and Andrew Morris.

2. Implementation of cyber risk mitigation strategies

Areas examined

The ANAO assessed whether the Department of the Treasury (Treasury), National Archives of Australia (National Archives), and Geoscience Australia were compliant with the Top Four mitigation strategies, were cyber resilient and had considered an implementation position for the additional four strategies recommended in the Essential Eight.

Conclusion

Of the three entities, only Treasury was compliant with the Top Four mitigation strategies and cyber resilient. National Archives was not compliant with the Top Four mitigation strategies but had sound ICT general controls and so was assessed as not cyber resilient but internally resilient. Geoscience Australia was not compliant with the Top Four mitigation strategies and did not have sound ICT general controls so was assessed as vulnerable to cyber attacks. All three entities had implemented only one of the four non-mandatory mitigation strategies in the Essential Eight, and were not well progressed in considering an implementation position for the other three strategies.

Area for improvement

The ANAO recommended that Geoscience Australia and National Archives establish arrangements to achieve compliance with the Top Four mitigation strategies (paragraph 2.15).

Were entities compliant with the Top Four mitigation strategies?

Treasury complied with the requirements of the Top Four mitigation strategies, while National Archives and Geoscience Australia did not comply. National Archives met the requirements for two of the strategies, patching ICT applications and minimising privileged user access, but not for application whitelisting or patching operating systems. Geoscience Australia was not compliant with any of the four strategies.[a]

Note a: Geoscience Australia had recently reassessed its cyber security arrangements and commenced an IT program of work to achieve compliance with the Top Four mitigation strategies, including deploying application whitelisting for critical ICT infrastructure, by late 2018.

Entity compliance with the Top Four mitigation strategies

2.1 As outlined in Chapter 1, the Top Four mitigation strategies are application whitelisting, application patching, operating system patching and minimising privileged user access.

2.2 Treasury was compliant with the requirements for implementing each of the Top Four mitigation strategies, and therefore met the mandatory requirements set out in the *Protective Security Policy Framework*. National Archives was compliant with two of the four mitigation strategies, and Geoscience Australia was not compliant with any of the four strategies.

2.3 Table 2.1 shows the ANAO's assessment of the three entities' compliance with the Top Four mitigation strategies, as at February 2018. The assessment was based on an aggregated score for the assessment of a number of controls for each of the four strategies, as discussed in Appendix 2.

Table 2.1: The ANAO's assessment of entities' compliance with the Top Four mitigation strategies

Control areas assessed	Assessment results		
	Treasury	National Archives	Geoscience
Application whitelisting			
Patching applications			
Patching operating systems			
Minimising privileged user access			

KEY:

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

Source: ANAO analysis.

Application whitelisting

2.4 Application whitelisting protects ICT systems against unauthorised applications running on them. Its purpose is to protect systems and networks from harmful applications. The Top Four mitigation strategies include the requirement for entities to implement application whitelisting for desktops and servers.

2.5 The ANAO assessed:

- Treasury as having effectively implemented application whitelisting on desktops and servers using a combination of approved whitelisting methods covering executables, software libraries and installers. The department also used monitoring tools in high risk business areas to report any attempts to bypass the application whitelisting policy;
- National Archives and Geoscience Australia as not sufficiently implementing application whitelisting to comply with the requirements of the Information Security Manual:
  - National Archives had only implemented application whitelisting on desktops. At the time of the audit, it had not completed a risk assessment nor had plans to implement application whitelisting on its servers[25]; and
  - Geoscience Australia did not have application whitelisting in place across its ICT environment at the time of audit fieldwork, although it had an IT program of work

25 National Archives advised that it had interpreted the Information Security Manual control quite literally, and only performed application whitelisting on Standard Operating Environment-based systems, which includes desktops and laptops. Servers were not included, as they do not have a Standard Operating Environment. National Archives advised that it is now aware that servers are in scope and will include application whitelisting of servers.

to review its cyber security posture—with regard to application whitelisting—for critical ICT infrastructure.[26]

2.6 None of the three entities had a documented and endorsed application whitelisting strategy. In practice, Treasury and National Archives relied on their respective Information Security Policy to document the requirement to deploy application whitelisting across the ICT environments. Their security policies were silent on strategies and practices for explicitly selecting and permitting software execution or network communication to deliver services and business requirements, and the preferred security protocol.[27]

2.7 Treasury and National Archives also used proprietary application whitelisting configuration software and security information and event management (SIEM) software as a secondary control to monitor, capture and log unauthorised attempts to install applications by general and privileged user accounts.

Patching applications and operating systems

2.8 The Top Four mitigation strategies include a requirement for entities to deploy security patches as soon as possible after being released by the vendor to protect ICT systems from known vulnerabilities. Critical security patches should be deployed within 48 hours from vendor release.[28] According to the Australian Signals Directorate, applying security patches to applications, operating systems and devices is one of the most effective security practices to address known system vulnerabilities.

2.9 Entities had installed either Microsoft Windows 7 or Windows 10 operating systems on their desktops. Entities used vendor provided tools to support the automatic deployment of security patches to desktops. The automated deployment of security patches was efficient and timely.

2.10 The ANAO assessed:

- Treasury as having adequately implemented patching of applications and operating systems. The department had a patch management practice that included deployment of patches, rollback and contingency in the event the patch failed, and expected timeframes to patch applications and operating systems. Treasury deployed security patches using automated processes on a monthly cycle for desktops and servers, and critical security patches were deployed within 48 hours from vendor release.[29]
- National Archives as having implemented patching of applications in accordance with the requirements of the *Protective Security Policy Framework*, but not patching of operating systems. National Archives deployed security patches for applications on a monthly cycle for desktops; and, in general, also for servers, although there were instances where patches were installed on a quarterly cycle. Less than 20 percent of critical operating

26 Geoscience Australia had compensating controls to prevent users from installing and running unauthorised applications on their desktops. The ANAO considered these compensating controls marginally adequate for general users, and inadequate in preventing unauthorised application installations by system administrators.

27 The Australian Signals Directorate mandates an approved application whitelisting method covering executables, software libraries, scripts and installers; and for higher risk environments hashed-based whitelisting.

28 Australian Signals Directorate 2017, *Australian Government Information Security Manual: Controls* [Internet], Commonwealth of Australia, available from <https://www.asd.gov.au/publications/Information_Security_Manual_2017_Controls.pdf> [accessed 7 December 2017].

29 Eleven per cent of the servers were manually patched.

system patches were deployed within 48 hours from vendor release across the server fleet. In addition, some servers were running operating systems that were out of vendor support, so that patches were no longer being released to address vulnerabilities.

- Geoscience Australia as not implementing patching of applications or operating systems in compliance with the requirements of the *Protective Security Policy Framework*. Geoscience Australia was inconsistent with its patching procedures, installing some security patches on a monthly cycle but not installing other patches at all. Most critical patches were installed between 7 and 30 days after vendor release—greatly exceeding the requirement to install critical patches within 48 hours, as specified in the Top Four mitigation strategies and the contractual agreement with the service provider.[30]

2.11 For all entities, system management software such as System Centre Configuration Manager was used to provide patching status reports. National Archives and Geoscience Australia had no procedures in place to verify the installation of security patches, including documented processes to investigate, resolve and reinstall security patches to applications, operating systems and devices.

Minimising privileged user access

2.12 Misuse of privileged access[31] can lead to significant security compromises, such as unauthorised information disclosure and system/process breakdown. The Top Four mitigation strategies include a requirement for entities to implement effective controls over assigning and using privileged accounts to maintain system and information integrity.

2.13 All entities had policies and procedures in place to enforce key controls over the use of privileged accounts, including:

- granting and restricting privileged accounts only to appropriate staff to meet role-based needs;
- minimising the number of privileged accounts;
- preventing privileged accounts from accessing emails and the Internet;
- passphrase length and complexity requirements; and
- activity logging and monitoring.

2.14 For all entities, the process of granting and revoking privileged user accounts is in accordance with the Information Security Manual. However, Geoscience Australia did not effectively manage privileged accounts, in particular for non-Windows application servers, where there was limited visibility of user access and activities. For all entities, while event logs were captured and stored, there was room to improve the active monitoring of privileged user accounts. The entities were aware of this shortfall and were reviewing strategies to address it.

30 Geoscience Australia's ICT operations are managed by DXC Technology (DXC) as the contracted ICT service provider. DXC is responsible for maintaining the security of ICT environment, including patch management. While DXC is responsible for ICT operations and security, Geoscience Australia remains accountable for its ICT security, including the administration and oversight of the service level agreement with DXC.

31 Privileged access can give a user the ability to: change key system configurations and control parameters; circumvent security measures; access sensitive information (such as audit and security); and access and modify data, files and accounts used by other users.

Recommendation no.1

2.15 Geoscience Australia and National Archives of Australia each establish a plan and timeframe to achieve compliance with the Top Four mitigation strategies, and monitor delivery against that plan.

Geoscience Australia's response: *Agreed.*

2.16 *We have already commenced actions to improve compliance to address the security issues identified including: the engagement of a senior consultant to advise on an overarching security framework; the establishment of a Security Working Group; and an action plan to address compliance with the Australian Signals Directorate's Strategies to mitigate cyber security incidents*.

National Archives of Australia's response: *Agreed.*

2.17 T*he National Archives agrees with the recommendation, and advises that a program of work will be planned in 2018–19, with monitoring of delivery to be managed internally and included in the Archives' mandatory compliance reporting. This program of work will include the activities to support application whitelisting and patching of operating systems*.

Were entities cyber resilient?

Of the three entities, only Treasury was cyber resilient, with a high level of protection from external intrusions and internal breaches. The department complied with the Top Four mitigation strategies and had sound ICT general controls in place for logical access and change management. The ANAO assessed National Archives as internally resilient but vulnerable to attacks from external sources. Geoscience Australia was assessed as vulnerable, with a high level of exposure and opportunity for external attacks and internal breaches and unauthorised disclosures of information.

2.18 Cyber resilience is the ability to continue providing services while deterring and responding to cyber attacks. Cyber resilience also reduces the likelihood of successful cyber attacks. To become cyber resilient, an entity must first establish effective ICT general controls. Effective ICT general controls provide a stable and reliable foundation upon which other processes and controls can be built. An entity must also effectively implement the Top Four mitigation strategies. Together, these form the basis of the entity's cyber resilience—in essence, how well the entity is protecting its exposure to external vulnerabilities and intrusions, internal breaches and unauthorised information disclosures, and how well it is positioned to address cyber threats.

2.19 ICT general controls are entity-wide structures, policies, procedures, and standards applied to information systems that support business processes.[32] They include controls over ICT governance, ICT infrastructure, security and access to operating systems and databases, application acquisition and development, and ICT change procedures. Effective implementation of ICT general controls provides a level of assurance that an entity's systems are protected from security threats.[33]

32 ANAO Audit Report No.15 2015–16 *Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2015*, p. 24.

33 ANAO Audit Report No.37 2015–16 *Cyber Resilience*, p. 28.

Two elements of the ICT general controls framework—logical access control and change management—are crucial as they relate directly to security management.[34]

2.20 Table 2.2 shows the ANAO's assessment of entities' ICT general controls.

Table 2.2: The ANAO's assessment of entities' ICT general controls

Control areas assessed	Assessment results		
	Treasury	National Archives	Geoscience
Logical access controls	▲	▲	▲
ICT change management	▲	▲	▲

KEY:

▲ Control objective ***not*** met. ▲ Identified control ***not*** in place but compensating controls in place and observed. ▲ Control objective is met.

Source: ANAO analysis.

2.21 Treasury and National Archives had effective ICT general controls in place, with effective controls for endorsing changes to ICT systems and adequate logical access controls. Geoscience Australia did not have effective ICT general controls due to weaknesses in logical access controls. All entities had effective controls for managing ICT changes.

2.22 With respect to logical access controls:

- Treasury had documented processes and procedures, including for passphrase length and complexity requirements. Based on sample testing, privileged user accounts were granted authorisation based on roles and job duties, although regular reviews to revalidate privileged user accounts were not conducted which led to a high number of privileged accounts.
- National Archives had processes and procedures, including for granting and revoking user access and for directly attributing shared accounts to a user, but there was room for improvement in managing privileged user accounts.
- Geoscience Australia had policy and procedures in place to support the management of user access, however user access controls were not effectively implemented at the database and operating system level.

2.23 All entities had controls in place to enforce the 'least privilege principle' over privileged users. The least privilege principle is to assign users with the minimal required system access rights that are necessary to support them performing their defined job duties. The National Archives and Geoscience Australia did not effectively implement the administration of privileged user accounts, particularly in segregating administrative access based on job duties. In some instances, privileged user accounts were not blocked from accessing the Internet and emails, and were not adequately monitored.

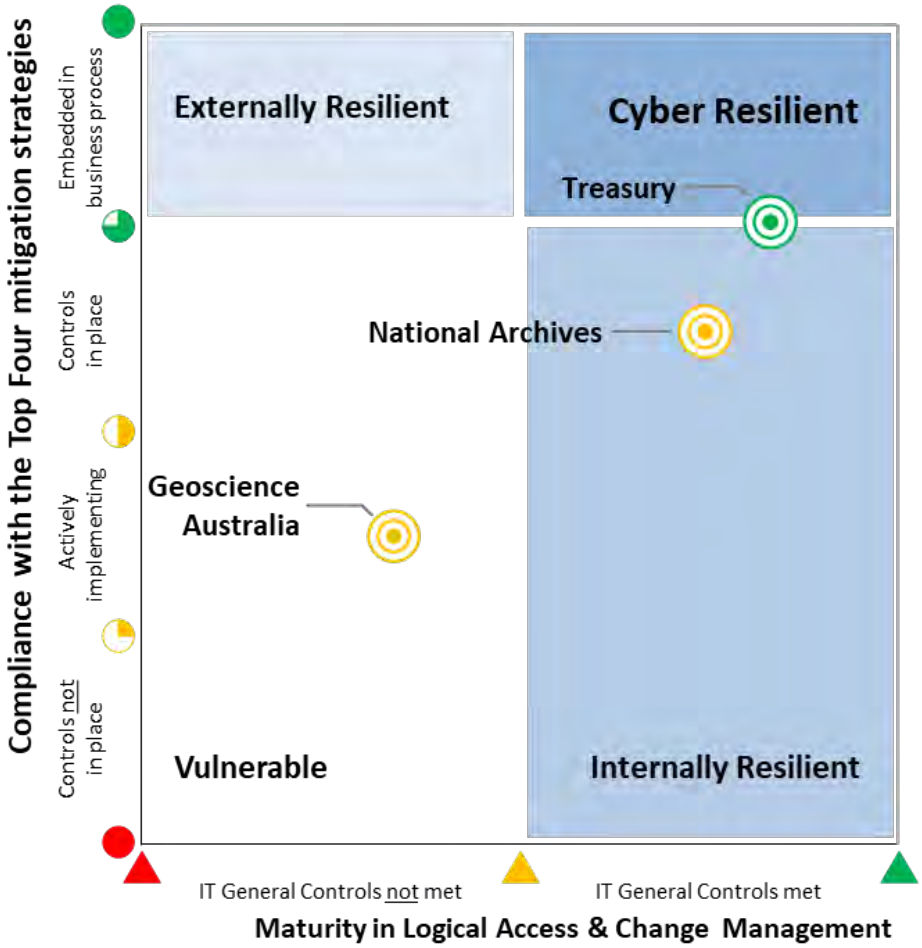
34 ibid. As discussed previously, logical access controls are tools and protocols used for identification, authentication, authorisation, and accountability in ICT systems.

2.24 All entities demonstrated maturity in the administration of change management. Changes to ICT systems required endorsements from responsible parties and testing before being implemented in the production environments. For the majority of change requests selected for testing, rollback plans were in place and appropriately documented.

Entity cyber resilience—summary assessment

2.25 Figure 2.1 summarises the ANAO's assessment of the entities' cyber resilience, which comprises compliance with the Top Four mitigation strategies and effective implementation of ICT general controls.

Figure 2.1 Entities' cyber resilience[a]



KEY:

- Control ***not*** in place and ***no*** dispensation authorised by the Accountable Authority.
- Control ***not*** in place but a dispensation is authorised by the Accountable Authority.
- Control ***not*** in place but entity is actively implementing, with a minimum of design deliverables in evidence.
- Control in place and meeting control objectives.
- Control in place and maintenance is part of business processes, including monitoring and taking corrective action as required.
- Control objective ***not*** met.
- Identified control ***not*** in place but compensating controls in place and observed.
- Control objective is met.

Note a: An entity's position on the matrix indicates its overall cyber resilience—in essence how well the entity is protected from external intrusions, internal breaches and unauthorised disclosures of information, and how well it is positioned to address threats.

Source: ANAO analysis.

2.26 Treasury is in the *Cyber Resilient* zone. Security controls are in place to provide a high level of protection from external attacks and internal breaches, and unauthorised disclosures of information. Treasury had achieved compliance with the requirements of the *Protective Security Policy Framework* to implement the Top Four mitigation strategies for cyber intrusions and threats.

2.27 National Archives is in the *Internally Resilient* zone. Security controls are in place to provide an adequate level of protection from breaches and disclosures of information from internal sources but vulnerabilities remain to attacks from external sources. The Top Four mitigation strategies are not in place across the ICT systems, or are inconsistently implemented across the systems. ICT general controls for logical access and change management are effective.

2.28 Geoscience Australia is in the *Vulnerable* zone. The Top Four mitigation strategies and ICT general controls are not in place or insufficiently implemented across the ICT systems.

2.29 National Archives and Geoscience Australia did not achieve compliance with the *Protective Security Policy Framework* requirement to implement the Top Four mitigation strategies.

Have entities implemented the four non-mandatory strategies in the Essential Eight?

The three entities had each implemented one of the four non-mandatory strategies in the Essential Eight—daily backup of important data. Treasury, National Archives and Geoscience Australia had made limited progress in implementing the other three non-mandatory strategies—disabling untrusted Microsoft Office macros, user application hardening and multi-factor authentication. In a few instances, the entities had considered risks and commenced developing plans to implement controls as part of the non-mandatory strategies, but were generally not well progressed in determining an implementation position for the strategies.

2.30 As discussed in paragraph 1.4, the four non-mandatory mitigation strategies in the Essential Eight are: disabling untrusted Microsoft Office macros; user application hardening; multi-factor authentication; and daily backup of important data, systems and configuration settings.

2.31 These controls are not mandatory and the Australian Signals Directorate has been actively promoting them as strategies to improve cyber resilience since February 2017. For the purposes of this audit, the ANAO assessed the extent to which the four non-mandatory mitigation strategies had been implemented (recognising that they need not be), and examined the plans and processes entities had put in place to consider implementing those strategies.

2.32 As shown in Table 2.3, none of the three entities had fully implemented the four non-mandatory strategies in the Essential Eight. All three entities had implemented one of the strategies—daily backup of important data.

Table 2.3: The ANAO's assessment of entities' compliance with the non-mandatory mitigation strategies in the Essential Eight

Control areas assessed	Assessment results		
	Treasury	National Archives	Geoscience
Disabling untrusted Microsoft Office macros	◑	◑	◑
User application hardening	◑	◑	◔
Multi-factor authentication	◔	◔	◑
Daily backup of important data	◕	◕	◕

KEY:

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

Source: ANAO analysis.

Disabling untrusted Microsoft Office macros

2.33 Configuring Microsoft Office macro settings addresses adversaries attempting to run malicious code while evading basic email content filtering and application whitelisting. Effectively configured macro settings for Microsoft Office should only allow macros vetted as trustworthy, and preferably placed in 'trusted location' directories in the entity's ICT environment with no write access for general and low-privileged user accounts. All other macros from the Internet that are not vetted should be blocked.

2.34 In all cases entities had implemented limited controls of Microsoft Office macros using configuration settings, and users were able to bypass these restrictions to run a macro. Entities did not adopt a risk-based approach to assess end-user functionalities against job needs. Rather, the entities adopted a 'one-size-fits-all' approach to setting restrictions on running Microsoft Office macros using configuration settings.

2.35 Entities advised the ANAO that they understood the importance of blocking untrustworthy macros but had to maintain end-user functionality so that staff were not disrupted in performing

their job duties. The three entities had not conducted a risk assessment, developed plans to implement effective controls for this mitigation strategy, or otherwise set out a rationale for not implementing an effective mitigation strategy.

User application hardening

2.36 Malicious content and Internet advertising accessed through web browser software can be reduced by disabling unneeded features in Microsoft Office, and by configuring web browsers to block Adobe Flash, ActiveX and untrusted Java code.

2.37 Treasury had configured the Internet gateway to block Adobe Flash from external web sites but applications on their network could run Adobe Flash files, for example training course material that relies on these features. Geoscience Australia and National Archives had no restrictions to run Adobe Flash from external web sites. All entities had limited controls to restrict untrusted Java code.

2.38 Entities had not assessed the effectiveness of the user application hardening controls and had no policy and procedures in place for applying appropriate security requirements. Instead entities relied on regular security patching of applications, such as Java, to maintain end-user applications and reduce the risk exposure.

Multi-factor authentication

2.39 Multi-factor authentication requires an authorised user to provide at least two of the following three mechanisms to gain access to an ICT system:

- something the user *knows*, such as a passphrase;
- something the user *has*, such as a physical token or software-based certificate; and
- something the user *is*, such as their fingerprint.

2.40 If implemented correctly, multi-factor authentication makes it more difficult for adversaries to use stolen user credentials to gain access to ICT systems to facilitate malicious activities.

2.41 All entities were using multi-factor authentication for remote access to ICT environments and, in addition to passphrases, have in place additional authentication methods recommended by the Information Security Manual.[35]

2.42 Treasury and National Archives did not have in place multi-factor authentication for privileged user accounts or any plans to implement this authentication. At the time of audit fieldwork, Geoscience Australia had multi-factor authentication in place only for system administrators with access to critical infrastructure systems on the cloud computing environment, and had an ICT program of work underway to deploy multi-factor authentication on key systems for all cloud application user accounts.

Daily backup of systems and data

2.43 Backup of systems and data is a common practice by organisations to ensure the resumption of normal information processing in the event of disruption to the ICT systems, such as through user error or failures of storage hardware. Given vulnerabilities and emerging cyber threats, recent

35 The Australian Signals Directorate recommends the following authentication methods: U2F security keys, physical tokens, biometrics and/or smartcards.

backup of data and proven data restoration processes are also vital to mitigate data being encrypted, corrupted or deleted by ransomware and other destructive malware.

2.44 The principle for data backups is:

- *frequency*—daily backups of operational data, and more frequently for important data;
- *reliable backup processes*—supported by a means to test the data afterwards to ensure that the process is actually recording all of the data onto the target backup device;
- *secure storage*—in a location (both physical and virtual environments) that is safe from unauthorised access and protected by ICT security controls such as encryption; and
- *restoration*—a documented and regularly tested process for restoring the backup.

2.45 All entities had backup policies and procedures in place, and conducted daily backup of their important data.[36] All entities stored backups for over three months, both onsite and offsite (physical environment) and using cloud computing services (virtual environment).

2.46 None of the three entities had formal procedures in place to test the restoration of backups. However, Geoscience Australia restored production backups to its test environment monthly, while Treasury and National Archives relied on operational restoration requests as a testing mechanism for their backups.

36 The ANAO limited its audit fieldwork to data backups conducted on the production environment.

3. Self-assessment and maturity model

Areas examined
The ANAO examined whether the three entities had accurately self-assessed and reported their compliance with the Top Four mitigation strategies. The ANAO also examined the application of the *Essential Eight Maturity Model*.

Conclusion
Two entities had accurately self-assessed and reported their level of compliance with the Top Four mitigation strategies, and the other entity had not. There are shortcomings in the *Essential Eight Maturity Model* that limits its usefulness in its current form, and could lead to entities inadvertently overstating their cyber security compliance if it is used in performing the self-assessment. With activities underway to revise security reporting under the *Protective Security Policy Framework,* it is timely to also strengthen guidance supporting entities to self-assess compliance with the mandatory mitigation strategies and processes to verify the correctness of those assessments.

Area for improvement
The ANAO recommended that the Attorney-General's Department, Department of Home Affairs and Australian Signals Directorate strengthen: guidance supporting entities to self-assess compliance with the Top Four mitigation strategies; processes to verify the correctness of those assessments; and transparency and accountability for compliance (paragraph 3.39).

Did the entities appropriately assess and report against compliance with the Top Four mitigation strategies?

All three entities conducted self-assessments against the Top Four mitigation strategies and reported their compliance in accordance with government requirements. Treasury and Geoscience Australia accurately assessed their level of compliance. National Archives incorrectly reported compliance against two strategies. In conducting the self-assessments, the entities did not have access to comprehensive guidance or supporting tools, such as control assessment test plans or grading schemes, which would have assisted accurate self-assessments according to the requirements of the *Protective Security Policy Framework*.

Annual self-assessment against the *Protective Security Policy Framework*

3.1 As discussed in Chapter 1, entities are required to undertake an annual self-assessment against the mandatory requirements of the *Protective Security Policy Framework*, and report the results to the relevant Portfolio Minister, Secretary of the Attorney-General's Department and Auditor-General.

3.2 The requirements for entities' self-assessment against the mandatory requirements of the *Protective Security Policy Framework* are divided into four categories:

- Governance (GOV), to implement and manage protective security governance arrangements;
- Personnel Security (PERSEC), to ensure the suitability of personnel to access Australian Government resources;

- Information Security (INFOSEC), to ensure the confidentiality, availability and integrity of all official information; and
- Physical Security (PHYSEC), to ensure a safe working environment for employees, contractors, clients and the public, and to provide a secure environment for official assets.

3.3 The Top Four mitigation strategies form part of INFOSEC 4, one of the mandatory requirements of the *Protective Security Policy Framework* under the Information Security category. According to the Attorney-General's Department's *Protective Security Policy Framework* Compliance Reports from 2014–15 to 2016–17, INFOSEC 4 had the highest rate of self-assessed non-compliance. In 2016–17, only 60.2 per cent of non-corporate Commonwealth entities reported compliance with the Top Four mitigation strategies.[37] This is despite the Top Four mitigation strategies representing the minimum requirements for entities. The three ANAO cyber security performance audits found higher rates of non-compliance—eight of the 11 entities assessed were not compliant with INFOSEC 4.

Self-assessments of the three audited entities

3.4 Table 3.1 presents the entities' self-assessment of compliance with the Top Four mitigation strategies as at July 2017; and the ANAO's rating of entity compliance as at March 2018.

Table 3.1: Entities' self-reported compliance ratings for the Top Four mitigation strategies, and the ANAO's ratings of entity compliance

Control areas assessed	Entities' self-reported compliance ratings at July 2017, and the ANAO's ratings of entity compliance at March 2018					
	Treasury		National Archives		Geoscience	
	Entity rating	ANAO rating	Entity rating	ANAO rating	Entity rating	ANAO rating
Application whitelisting	● a	●	●	●	●	●
Patching applications	●	●	●	●	●	●
Patching operating systems	●	●	●	●	●	●
Minimising privileged access	●	●	●	●	●	●

KEY: ● Compliant ● Not compliant

Note a: Treasury reported that it was compliant for application whitelisting for the desktop, and non-compliant for servers although mitigation controls were in place. During audit fieldwork the department completed its ICT program of work to implement application whitelisting on the servers.

Source: Entities' 2017 annual self-assessment report against the *Protective Security Policy Framework* and ANAO analysis.

3.5 In the July 2017 self-assessment for compliance and reporting to government:

- Treasury self-assessed as compliant for three of the Top Four mitigation strategies;
- National Archives of Australia self-assessed as fully compliant with the strategies; and

37 Self-reported compliance with INFOSEC 4 for non-corporate Commonwealth entities increased from 48.4 per cent in 2014–15 to 59.1 per cent in 2015–16 and 60.2 per cent in 2016–17—an increase of 11.8 percentage points over the period, mainly achieved in 2015–16.

- Geoscience Australia self-assessed as non-compliant.

3.6 As at March 2018, the ANAO assessed that:

- Treasury was compliant with each of the Top Four mitigation strategies. The ANAO's higher compliance rating for application whitelisting stemmed from the different timing of the assessments. The department completed a program of work to implement application whitelisting on servers in February 2018, which was after its self-assessment, but before the ANAO's assessment and critical to the outcome;
- National Archives was not compliant with two of the Top Four mitigation strategies; and
- Geoscience Australia was not compliant with any of the Top Four mitigation strategies.

3.7 The self-assessments and ANAO assessments were consistent for Geoscience Australia and Treasury (after adjusting for the timing difference) but not for National Archives. Accordingly, the ANAO considers that Treasury and Geoscience Australia accurately assessed and reported the level of compliance with the Top Four mitigation strategies as part of the 2017 reporting against the mandatory requirements of the *Protective Security Policy Framework,* but National Archives incorrectly reported compliance and should have reported non-compliance.

Entities' self-assessment processes

3.8 In conducting annual self-assessments against the mandatory requirements of the *Protective Security Policy Framework,* entities relied on:

- an assessment conducted by those with prime responsibility for cyber security, such as the Information Technology Security Advisor;
- an assessment conducted by an external ICT security advisor, as requested by the Chief Information Security Officer or Audit Committee; and/or
- past ICT operations reports, as submitted by the ICT divisions or contracted ICT service providers.

3.9 The ANAO sought documented information from the three entities about their assessment of the Top Four mitigation strategies and found that reported statements for compliance could not be substantiated with evidence. In most cases, entities relied on control assessment reports that were greater than six months from the time of reporting to government. In particular, Treasury and National Archives could not provide the evidence used and analysis created to inform their compliance self-assessments. This indicates insufficient senior management oversight and challenge of the assessment of achieving compliance with the Top Four mitigation strategies.

3.10 Where entities' controls were assessed as non-compliant, there were no documented initiatives to achieve compliance. For example, Geoscience Australia had an ICT security assessment conducted by the Australian Signals Directorate in July 2016. The overall findings from the assessment were that the entity was non-compliant with the mandatory mitigation strategies. The Chief Executive Officer accepted the cyber risks. No further assessments of cyber risks or planned cyber initiatives were taken until 2017.[38]

38 An internal audit on INFOSEC compliance was completed in June 2017, and Geoscience Australia subsequently amended policy statements.

3.11 As previously discussed, the aim of the *Australian Government Information Security Manual* is to detail the technical security controls that can be implemented to help mitigate security risks to entities' information and systems. The manual is silent in detailing the preferred criteria and methodology for assessing the operating effectiveness of controls.

3.12 Entities must rely on professional judgement—from internal and/or external ICT security advisors—to assess security controls' effectiveness. Different approaches and interpretations of the assessment criteria will continue in the absence of a common control assessment methodology.

3.13 The Australian Signals Directorate has issued implementation guidance for the Essential Eight in its supplementary document to the *Information Security Manual*.[39] There is no similar guidance or supporting information, including assessment and reporting tools such as control assessment test plans, for the annual self-assessment processes.

3.14 There was also not a grading scheme that reflects the security control operating effectiveness. The current rating of either compliant or non-compliant is limited, and may not accurately reflect an entity's adequacy of implementation and control effectiveness for their ICT environment.

3.15 In the absence of a common control self-assessment methodology and guidance, including a broader grading scheme, entities may continue to inaccurately self-assess and report on the adequacy of security controls.

3.16 A common control self-assessment methodology, supported by appropriate guidance and grading scheme is required to:

- achieve consistent management of cyber risks and cyber investments (*entity-level*); and
- strengthen trust online and protect Australian's privacy and Australia's social, economic and national interests (*government-level*).

Can the Essential Eight Maturity Model be used to assess maturity in implementing the Essential Eight?

In its current form, the *Essential Eight Maturity Model* is unlikely to achieve its objective of assisting entities to determine their maturity in implementing the Essential Eight mitigation strategies. This is primarily because there is inconsistent and incomplete alignment between the definitions of mitigation strategies in the *Australian Government Information Security Manual* and the criteria for attaining a particular maturity level in the *Essential Eight Maturity Model* document.

A revised *Protective Security Policy Framework* and updated reporting requirements is scheduled for 2018–19. In light of the continued low level of compliance with the Top Four mitigation strategies, the revised framework should incorporate adequate technical guidance to support entities to accurately self-assess against those strategies, additional verification of compliance with those requirements and enhanced transparency about entities' compliance.

39 Australian Signals Directorate, *Strategies to Mitigate Cyber Security Incidents—Mitigation Details*, 2017.

3.17 To assist entities in determining their maturity in implementing the Essential Eight mitigation strategies, the Australian Signals Directorate has prepared an *Essential Eight Maturity Model*.[40] The model has five levels of maturity, broadly defined as:

- *Maturity Level Zero*—not aligned with intent of mitigation strategy;
- *Maturity Level One*—partly aligned with intent of mitigation strategy;
- *Maturity Level Two*—mostly aligned with intent of mitigation strategy;
- *Maturity Level Three*—fully aligned with intent of mitigation strategy; and
- *Maturity Level Four*—for higher risk environments fully aligned with intent of mitigation strategy.[41]

3.18 According to the Australian Signals Directorate, entities not operating in higher risk environments should aim to reach a maturity level of three for all of the Essential Eight mitigation strategies.[42] This maturity level rating would equate to compliance with the requirements of the strategies for those entities. This rating would mean that the entities have satisfied the minimum requirements for mitigating cyber risks through the Top Four strategies, and satisfied the additional four strategies of the Essential Eight that are not mandatory.

3.19 The minimum criteria required to be met for Maturity Level Three for each mitigation strategy is presented in Appendix 3.

3.20 The ANAO assessed each of the three entities' maturity according to the *Essential Eight Maturity Model*, and compared it to the assessment of compliance with the Top Four and additional four mitigations strategies, as reported in Chapter 2.

3.21 This assessment highlighted that the criteria used to determine the levels of maturity in the *Essential Eight Maturity Model* are not closely aligned to the criteria used by the ANAO to determine the level of compliance with the Essential Eight mitigation strategies. The ANAO's criteria are based on the controls outlined by the Australian Signals Directorate in the *Australian Government Information Security Manual* and *Strategies to Mitigate Cyber Security Incidents*, for the purpose of supporting entities to comply with the requirements of the *Protective Security Policy Framework.*

3.22 Table 3.2 (application whitelisting) and Table 3.3 (restrict administrative privileges) present a comparison of the controls identified as mandatory for the implementation of two of the Top Four mitigation strategies, and identify which of these controls need to be implemented to achieve a maturity assessment of three. Appendix 4 includes a comparison of the remaining Top Four mitigation strategies.

---

40 The Australian Signals Directorate states that the *Essential Eight Maturity Model* document 'is intended for cyber security professionals looking to determine the maturity of their implementation of the Essential Eight mitigations strategies,' available from <https://www.asd.gov.au/publications/protect/essential-eightmaturity-model.htm> [accessed 8 January 2018].

41 Australian Signals Directorate, *Essential Eight Maturity Model*, October 2017, available from <https://www.asd.gov.au/publications/protect/essential-eight-maturity-model.htm> [accessed 19 June 2018].

42 Some organisations are constantly targeted by skilled adversaries, or otherwise operate in a higher risk environment. The Australian Signals Directorate recommends that these organisations reach a maturity level of four for their mitigation strategies.

Table 3.2: Application whitelisting: mandatory controls under the *Protective Security Policy Framework* and treatment in the *Essential Eight Maturity Model*

Row no.	Requirement of the Information Security Manual (ISM) and *Protective Security Policy Framework*	Included in Maturity Model?	Maturity rating
1	Agencies must use an application whitelisting solution within SOEs[a] to restrict the execution of programs and DLLs[b] to an approved set. [ISM 0843]	Yes	Maturity Level 3
2	Users and system administrators must not be allowed to temporarily or permanently disable, bypass or be exempt from application whitelisting mechanisms. [ISM 0846]	No	Not applicable
3	Agencies must implement application whitelisting using at least one of the methods: cryptographic hashes, publisher certificates, absolute paths, parent folders. [ISM 0955]	Yes	Maturity Level 4 (specifies use of only file hashes)
4	When implementing application whitelisting using parent folder rules, file system permissions must be configured to prevent users and system administrators from adding or modifying files in authorised parent folders. [ISM 1391]	No	Not applicable
5	When implementing application whitelisting using absolute path rules, file system permissions must be configured to prevent users and system administrators from modifying files that are permitted to run. [ISM 1392]	No	Not applicable
6	Agencies should use an application whitelisting solution within SOEs to restrict the execution of scripts and installers to an approved set. [ISM 1413 – however not identified as a mandatory control]	Yes	Maturity Level 3

Note a: SOE is Standard Operating Environment. This is the specification of the architecture, operating systems, application set and configuration of computers within an organisation.

Note b: DLL is Dynamic Link Library. This is a file that contains a library of functions and other information that can be accessed by a Windows program.

Source: ANAO analysis.

3.23 For application whitelisting, an assessment of Maturity Level 3 could be achieved with the implementation of only one of the five mandatory controls (Row 1 in Table 3.2), however it would also require the implementation of a control in the *Essential Eight Maturity Model* (Row 6) that is not mandatory under the *Protective Security Policy Framework*. Implementation of the second of the five mandatory controls (Row 3) would enable the entity to achieve a maturity assessment of four.

Table 3.3: Restrict administrative privileges: mandatory controls under the *Protective Security Policy Framework* and treatment in the *Essential Eight Maturity Model*

Row no.	Requirement of the Information Security Manual (ISM) and *Protective Security Policy Framework*	Included in Maturity Model?	Maturity rating
1	Agencies must: • limit system access on a need-to-know basis; • have any requests for access to a system authorised by the person's manager; • provide personnel with the least amount of privileges needed to undertake their duties; • review system access and privileges at least annually and when personnel change roles; and • when reviewing access, ensure a response from the person's manager confirming the need to access the system is still valid, otherwise access will be removed. [ISM 0405]	Partial (highlighted controls only)	Maturity Level 2 (annual review of privileges) Maturity Level 3 (annual review of privileges and duties-based restrictions)
2	Agencies must restrict the use of privileged accounts by ensuring that: • the use of privileged accounts are controlled and auditable; • system administrators are assigned a dedicated account to be used solely for the performance of their administration tasks; • privileged accounts are kept to a minimum; • privileged accounts are used for administrative work only; • passphrases for privileged accounts are regularly audited to check they meet passphrase selection requirements; • passphrases for privileged accounts are regularly audited to check the same passphrase is not being reused over time or for multiple accounts (particularly between privileged and unprivileged accounts); and • privileges allocated to privileged accounts are regularly reviewed. [ISM 0445]	No	Not applicable
3	Agencies must conduct the remote administration of systems, including the use of privileged accounts, over a secure communications medium from secure devices. [ISM 0985]	No	Not applicable
4	Agencies must prevent users from using privileged accounts to read emails, open attachments, browse the web or obtain files via internet services such as instant messaging or social media. [ISM 1175]	Yes	Maturity Level 1 (policy controls) Maturity Level 3 (technical controls)

Source: ANAO analysis.

3.24 For the strategy to restrict administrative privileges, an assessment of Maturity Level 3 could be achieved with implementation of one (Row 4 of Table 3.3) and partial implementation of a second of four controls (Row 1) that the *Protective Security Policy Framework* identifies as being mandatory for this strategy.

3.25 In the case of all four mandatory strategies, the mandated controls that make up each strategy are included at Appendix 6. It would be possible to achieve a maturity rating of three under the *Essential Eight Maturity Model* without implementing all of these controls. The ANAO considers that some of these controls, if not implemented, would undermine the effectiveness of the strategies—for example, the control to prevent users from bypassing the whitelisting mechanism.

3.26 In the case of application whitelisting, an entity could achieve compliance with the strategy but not be assessed as achieving Maturity Level 3 (because it does not satisfy a non-mandatory control under the *Protective Security Policy Framework*—Row 6 in Table 3.2).

3.27 In its current format, the *Essential Eight Maturity Model* does not provide a means for entities to accurately assess compliance. If entities also use the model in self-assessing and reporting on compliance with mandatory mitigation strategies, the potential exists that entities will overstate or understate compliance, make incorrect and inefficient cyber security investment decisions and inadequately mitigate cyber risks.

3.28 Given the multiple instruments in assessing the effectiveness of ICT security controls, there is likely to be uncertainty for entities in deciding whether to adopt: a controls-based assessment by using the Information Security Manual; or the simpler *Essential Eight Maturity Model*, which may not provide the required level of assurance.

Compliance arrangements for cyber security

3.29 Responsibilities for cyber security in the Commonwealth are with the Accountable Authorities of the particular Commonwealth entities for implementing effective cyber security arrangements in their entity, and various entities with broader responsibilities. These entities include:

- Attorney-General's Department, as the policy owners of the *Protective Security Policy Framework*;
- Department of Home Affairs, responsible for cyber security policy coordination; and
- Australian Signals Directorate, as regulator of the policy for promoting compliance with the Information Security Manual.

3.30 This audit has identified a lack of guidance for entities to self-assess and report against compliance with the Top Four mitigation strategies, and problems with the accuracy of the *Essential Eight Maturity Model* in assisting entities to determine compliance.

3.31 As discussed in paragraph 3.3 (and Appendix 5), each of the previous three ANAO audits on cyber security identified high rates of non-compliance with the requirements of the *Protective Security Policy Framework*. The findings in this audit are of similar levels of non-compliance with the Top Four mitigation strategies, and in total only four of the 14 entities assessed have been compliant. Self-reporting of compliance also remains low (at around 60 per cent).

3.32 The cyber security framework as it stands only contains reporting based on self-assessment as a compliance mechanism. Reports to the Secretary of the Attorney-General's Department are not made public, and are not used to inform further compliance activities by the Australian Signals Directorate. Audits by the ANAO are the only additional activity that provide transparency of compliance with the framework. Given the importance of managing cyber security, the current regulatory framework is not driving sufficient improvements in cyber security.

Changes to security reporting and cyber-related requirements under the Protective Security Policy Framework

3.33 Changes have been proposed to security reporting requirements under the *Protective Security Policy Framework.* The proposals include a requirement on 'safeguarding information from cyber threats' that explicitly identifies application whitelisting, application and operating system patching, and restricting administrative privileges as mandatory requirements of the *Protective Security Policy Framework*. In June 2018, the Government Security Committee is scheduled to consider supporting policy and guidance for this core requirement, that aims to more clearly articulate what is mandated for entities' application whitelisting, application and operating system patching, and restricting of administrative privileges (with reference to guidance in the Information Security Manual).

3.34 In consultation with entities, the Attorney-General's Department has developed a new approach to reporting against the *Protective Security Policy Framework*[43]*,* to address identified concerns about the accuracy of self-assessed reporting. There will be a revised *Protective Security Policy Framework* reporting template and additional assurance measures to support accurate self-assessments, including for the first time the need to have supporting evidence.[44] The existing compliant/non-compliant approach will be replaced by a broader maturity rating model comprised of four grading levels[45], with maturity indicators for each maturity level.

3.35 The ANAO has not audited the proposed maturity model or draft reporting template but notes that technical guidance has not yet been developed that would provide detailed control assessment test plans that are well aligned to the controls outlined by the Australian Signals Directorate for the Top Four Mitigation Strategies, and accurately reflect security control effectiveness. It is important that the Australian Signals Directorate develops such guidance to support the reporting changes underway.

3.36 The revised security reporting and cyber-related requirements under the *Protective Security Policy Framework* are scheduled to be implemented in 2018–19. In line with the Joint Committee of Public Accounts and Audit's Recommendation 4 of Report 456, after that time the ANAO would be in a position to consider conducting an audit of the effectiveness of the self-assessment and reporting regime under the *Protective Security Policy Framework.*

3.37 The changes underway to security reporting and cyber-related requirements under the *Protective Security Policy Framework* do not include any new proposals for verification of

43 The Attorney-General's Department has reviewed the framework and process for *Protective Security Policy Framework* reporting with the Government Security Committee agreeing a new *Protective Security Policy Framework* reporting model at its meeting of 13 December 2017. Supporting policy requirements and guidance material were agreed by the Committee at its March 2018 meeting for commencement from 1 July 2018.

44 These assurance mechanisms also include entities having to: demonstrate a cycle of security planning, monitoring and reporting each year; and explain how key security risks were managed.

45 These levels are ad hoc, developing, managing and embedding—and broadly align with the levels in the *Essential Eight Maturity Model*.

compliance. In light of the continued low level of compliance with the Top Four mitigation strategies, consideration should be given to also strengthening this aspect of the framework.

3.38 The proposed changes also do not include strategies or activities to improve the transparency of compliance with cyber security requirements or accountability for achieving or not achieving compliance—such as public reporting of the reports to the Secretary of the Attorney-General's Department.

Recommendation no.2

3.39 In revising security reporting and cyber-related requirements under the *Protective Security Policy Framework*, the Attorney-General's Department, Department of Home Affairs and Australian Signals Directorate work together to improve compliance with the framework by:

(a) providing adequate technical guidance to support entities to accurately self-assess compliance with the Top Four mitigation strategies and their underlying controls contained in the Information Security Manual;

(b) developing a program for verifying entities' reported compliance with the mandatory cyber security requirements; and

(c) increasing transparency and accountability about entities' compliance with those requirements.

Attorney-General's Department's response:

(a): *Agreed.*

3.40 *Proposed reforms to the Protective Security Policy Framework (PSPF), which are to take effect later this year, more clearly articulate the policy requirements for safeguarding information from cyber threats, as well as the links to underlying controls contained in the information security manual. The department notes the ANAO's paragraph 3.35 finding that 'it is important that the Australian Signals Directorate (ASD) develops such guidance (providing detailed control assessment test plans) to support the reporting changes underway'; the department agrees to support ASD in this work.*

(b): *Agreed in principle.*

3.41 *To support verification, the department's proposed reforms to the PSPF will introduce enhanced reporting obligations designed to provide greater assurance of the accuracy of entities' self-assessed reporting. For example, entities will be required to provide supporting evidence to demonstrate a cycle of security planning, monitoring and reporting each year, and explain how key security risks are managed*.

3.42 *Developing a verification program for cyber security is a matter for the Australian Cyber Security Centre. The department supports ASD and Department of Home Affairs considering possible further verification mechanisms and will provide assistance as appropriate.*

(c): *Agreed.*

3.43 The department acknowledges the importance of improving transparency and accountability. To support this, the department agrees to publicly release the 2017–18 consolidated annual whole-of-government Protective Security Compliance Report (and future maturity reports).

Australian Signals Directorate's response: *Agreed.*

3.44 *ASD agrees with Recommendation 2. ASD acknowledges the inconsistent mapping between the 2017 Australian Government Information Security Manual and the Essential Eight Maturity Model. ASD is currently consulting on proposed changes to address this in the 2018 Australian Government Information Security Manual and continues to work with the Attorney General's Department to ensure alignment with Protective Security Policy Framework reforms. While ASD provides cyber security advice to a variety of audiences, it remains the responsibility of Commonwealth entities to maintain a workforce of competent cyber security practitioners capable of assessing the effective implementation of security controls for their information and communication technology systems*.

3.45 *ASD agrees to continue working with the Attorney-General's Department and the Department of Home Affairs but notes that it is neither a regulatory body nor a compliance reporting agency. ASD works to provide better practice cyber security guidance to Commonwealth entities. ASD commends Commonwealth entities which achieve full compliance with mandatory requirement INFOSEC 4 from the Protective Security Policy Framework and also recognises the achievements of those making significant and sustained annual improvements to their cyber security posture*.

3.46 *ASD supports mature risk management frameworks for cyber security over compliance-based programs. Further, ASD encourages positive and sustained improvements to Commonwealth entities' cyber security posture over time. From experience we acknowledge that in some circumstances the application of all Top Four mitigation strategies may not be practicable, or introduces additional risks, and that other mitigating controls may achieve a similar outcome. ASD agrees to work with the Attorney-General's Department and the Department of Home Affairs to assist both entities further their compliance measurement goals*.

Department of Home Affairs response: *Agreed.*

3.47 *The Department of Home Affairs (Home Affairs) supports this recommendation. Home Affairs agrees there should be adequate technical guidance to support entities and a verification program for reported compliance. Home Affairs further supports the [ANAO's] view that there should be increased transparency and accountability regarding entities' compliance.*

3.48 Home Affairs will continue to work closely with the Australian Signals Directorate and Attorney General's Department to strengthen the standard of cyber security of Australian Government networks.

3.49 Home Affairs has responsibility for cyber security policy and coordination. In this capacity, Home Affairs will support the Attorney-General's Department efforts to update the Protective Security Policy Framework and the Australian Signals Directorate's efforts to update the Information Security Manual, including ensuring these policies are mutually supportive of the goal of improved cyber security standards across government.

3.50 Home Affairs supports the Attorney-General's Department undertaking to publish the 2017-18 consolidated annual whole-of-Government Protective Security Compliance Report (and future maturity reports).

3.51 Home Affairs will work with the Attorney-General's Department and the Australian Signals Directorate to develop a fit-for-purpose mechanism for verifying entities reported compliance and provide advice to the Secretaries' Cyber Security Board.

4. Management arrangements and cyber resilience culture

Areas examined

The ANAO assessed the effectiveness of the three entities' arrangements for managing cyber security risks, and aspects of their cyber resilience culture.

Conclusion

The three entities had partly effective arrangements for managing cyber security risks, with specialist staff in dedicated security positions contributing to existing ICT processes and broader business models. However, the entities did not adopt a risk-based approach to prioritise improvements to cyber security, with cyber security investments focused on short-term operational needs rather than long-term strategic objectives. Until the National Archives and Geoscience Australia achieve compliance with the mandatory strategies, it is inappropriate to consider that a positive cyber resilience culture is in place.

Background

4.1 As discussed in Chapter 1, JCPAA *Report 467: Cybersecurity Compliance* recommended that the ANAO outlines the behaviours and practices it would expect in a cyber resilient entity, and assesses against these in future audits of cyber security compliance.[46]

4.2 To address this recommendation, the ANAO has drawn on previous audit work to assess the cyber resilience culture of the three audited entities. In particular, this audit has drawn on ANAO Audit Report No.37 2015–16 *Cyber Resilience*, which included a list of behaviours and practices that may improve the level of cyber resilience (Table 3.1 on p. 41 of that report). These criteria have been refined and expanded upon to form the basis of the current assessment.

4.3 The ANAO also recognises that the Australian Signals Directorate and relevant policy entities (Attorney-General's Department and Department of Home Affairs) are responsible for security self-assessment and reporting processes, and, as such, are better positioned to articulate the appropriate cyber resilient behaviours and practices. If such criteria are incorporated into their guidance documents, the ANAO will reference that guidance in future cyber security audits.

Characteristics of a cyber resilient organisation

4.4 Robust and up-to-date technical security solutions alone cannot safeguard individuals' data and economic information stored by government entities. The implementation of the mandatory strategies, effectiveness of an entity's ICT general controls framework, and a fit for purpose cyber security culture forms the basis of its cyber resilience.

4.5 In 2015, the ANAO reported in its second cyber security performance audit that effective entities had a business model and ICT governance that incorporated ICT security into their strategy, planning and delivery of government services. For these entities, ICT systems were no longer considered an enabler to business—they were core business. These entities understood the risk profile across their enterprise ICT systems, and managed those risks systematically, including

46 JCPAA, *Report 467: Cybersecurity Compliance*, October 2017, p. viii.

through assessments of the effectiveness of controls and security awareness training. They had taken steps to improve business processes to accommodate the security strengths and weaknesses of each ICT system. For these effective entities, ICT security was a priority.

4.6 The deployment of ICT security measures does not in itself ensure a strengthened ICT security posture across the enterprise environment. Effective entities adopted a risk-based approach to identify and prioritise security enhancements and to ensure the highest vulnerabilities are addressed first. These entities had an integrated and documented architecture for data, systems and security controls, designed and deployed security measures at a system-level rather than at a control-level, and were aware of the importance of looking beyond the Top Four mitigation strategies. The entities had taken varying steps to implement the remaining strategies from the Australian Signals Directorate *Strategies to Mitigate Cyber Security Incidents.*[47]

4.7 Cyber resilient entities also demonstrate a leadership culture and behaviours that prioritise cyber security and focus on it, investing to strengthen their ICT environments to make the most of opportunities online. Executives and senior managers in these entities were informed of the cyber trends—the motives, opportunities and emerging technology—that might target and compromise their systems, and responded to cyber security incidents in a timely manner. These managers understood their roles and responsibilities for the business services and systems for which they were accountable. They did not expect ICT technical staff to be solely responsible for resolving ICT security matters.

4.8 Effective entities had key ICT operational staff with a sound understanding of the threats that may affect the enterprise ICT network, applications, databases and operating systems. They were aware of known security flaws affecting their assigned systems, and deployed mitigating controls in the absence of enterprise-wide security measures.

4.9 Security awareness and initiatives are a shared responsibility within an organisation. Entities that embedded security awareness as part of their culture adopted a mutual obligation approach towards security responsibility and accountability. All staff had a duty to monitor and report on observed cyber attacks. These entities had established ICT security officers[48], and provided information security awareness and training to all staff and contractors.

4.10 These characteristics of cyber resilient organisations have formed the basis of the ANAO's assessment of the three audited entities.

47 Australian Signals Directorate, *Strategies to Mitigate Cyber Security Incidents* [Internet], 2017, available from <https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-table.htm> [accessed 20 April 2018].

48 Key personnel are the Chief Information Security Officer, the Information Technology Security Advisor and the Information Technology Security Officers.

Did entities have effective arrangements in place for managing cyber risks?

The three entities had partly effective arrangements for managing cyber security risks, with scope for improvement in important elements of risk management and governance. Two of the three entities had established a business model and ICT governance that incorporated ICT security into strategy, planning and delivery of services, and all entities had key ICT operational staff with a sound understanding of the vulnerabilities and cyber threats that may affect their ICT systems. The three entities had not adopted a systematic risk-based approach to prioritise improvements to cyber security across their ICT systems, or identified and documented cyber initiatives beyond 2017–18, and key ICT security management roles had not been consistently filled.

4.11 The review of management arrangements to assess cyber resilience covered: risk management and governance arrangements; and risk-based processes for prioritising improvements to cyber security. In assessing the other behaviours and practices of a cyber resilient entity, the ANAO considered the entities' measures to build a culture of cyber resilience to fit their business needs.

Cyber security risk management and governance

4.12 Table 4.1 shows the ANAO's assessment of the three entities' cyber security risk management and governance arrangements.

Table 4.1: Entities' cyber security risk management and governance arrangements

Areas assessed for risk management and governance arrangements	Treasury	National Archives	Geoscience Australia
ICT security incorporated into strategy, planning and delivery of services	☑	☑	☑
Systematic approach to managing cyber risks, including assessments of the effectiveness of controls and security awareness training	☑	☑	☑
Integrated and documented architecture for data, systems and security controls	☑	☒	☒
Enterprise-wide governance arrangements	☑	☑	☑
Information security roles assigned and responsibilities communicated	☑	☑	☑
ICT operational staff understand the vulnerabilities and cyber threats to the system	☑	☑	☑

KEY: ☑ effective ☒ not effective ☑ area for improvement

Source: ANAO analysis.

4.13 Two of the three entities (Treasury and National Archives) had incorporated ICT security into strategy, planning and delivery of services. Their respective corporate plans and annual reports had documented key enterprise risks and cyber strategies to support the effective delivery of government services. Geoscience Australia advised in May 2018 that it had developed a plan to update its strategic and planning documents to better incorporate ICT security.

4.14 Entities provided evidence to demonstrate that a number of key cyber security practices were in place. These practices included managing key ICT infrastructure, conducting threat assessments before rolling out new ICT systems and conducting security awareness programs at staff induction and annually after that. In practice, each of the three entities had a range of non-systematic approaches to managing cyber risks across their operations that did not always align with the enterprise strategic initiatives.[49]

4.15 The ANAO expected entity business models and ICT governance to be informed by an integrated and documented architecture for data, systems and security controls, to ensure 'security by design' of the enterprise ICT systems. All three entities had a high-level enterprise-wide ICT systems architecture plan, but in two entities these plans were out-of-date and/or did not reflect the actual ICT systems design. Supporting documentation did not include: the security initiatives in use across the ICT systems and the effectiveness of the controls; and an endorsed storage strategy, outlining the business owner of the data, business importance of the data to the entity, and security classification of the data stored.

4.16 Each of the three entities had enterprise-wide governance arrangements in place, including risk management and business continuity frameworks, to manage their business and deliver government services.

4.17 According to Treasury, the department takes a deliberately cautious approach to managing risk, which it considers appropriate given the nature of its work. For example in preparing the annual Commonwealth Budget, the department conducts risk workshops in the lead up to the Budget period, including running desktop exercises for business continuity, disaster recovery and data backups. During the Budget preparation period, there is a 'freeze' on changes to the enterprise-wide ICT systems.

4.18 In all three entities, the audit and risk committees met regularly to review enterprise-level and operational-level risks, and focused on key delivery services and projects in-flight. There was no evidence that these committees reviewed vulnerabilities and cyber threats. For National Archives and Geoscience Australia, risk registers were prepared at the division or branch level but were not consolidated in an enterprise risk register to inform decision making on cyber risks and investments.

4.19 In all three entities, information security roles had been assigned to key positions and the responsibilities documented, however the positions were not all filled. At the time of audit fieldwork, Treasury had recently appointed a Chief Information Officer at the Senior Executive Service level to take on the role and responsibility of Chief Information Security Officer. Geoscience Australia had also recently appointed a Chief Information Officer at the Senior Executive Service level, and had separated that role from the Chief Information Security Officer position, with the Chief Operating Officer having responsibility for that role. The National Archives separated the roles of Chief Information Officer and Chief Information Security Officer in November 2017, appointing the Assistant Director-General Corporate Services to the latter role. National Archives was in the process of recruiting a Chief Information Officer at the time of the audit.

49 For example, Geoscience Australia's management of cyber security risks was not well aligned to its corporate risk management processes.

4.20 For all three entities, the frequent movement of experienced Chief Information Security Officers and Information Technology Security Advisors was a challenge. The ANAO considers that this increases the importance of a systematic rather than individual approach to cyber security—that can continue to be implemented and monitored by senior management even in the absence of ICT security management roles being filled.

4.21 The three entities had key ICT operational staff with a sound understanding of the vulnerabilities and cyber threats that may affect their ICT systems. In all entities, security awareness initiatives, including communication and training, were part of their culture. All staff had a duty to monitor and report on observed cyber threats.

Prioritising improvements to cyber security

4.22 Table 4.2 shows the ANAO's assessment of the three entities' initiatives and priorities to improve cyber security.

Table 4.2: Entities' initiatives and priorities to improve cyber security

Areas assessed for cyber security initiatives and priorities	Treasury	National Archives	Geoscience Australia
Adopted a risk-based approach to identify and prioritise cyber security improvements	☒	☒	☒
Prioritise cyber investments – short term (within two years)	☑	☑	☑
Prioritise cyber investments – long term (more than two years)	☒	☑	☒

KEY: ☑ effective ☒ not effective ☑ area for improvement

Source: ANAO analysis.

4.23 The three entities did not adopt a systematic risk-based approach to prioritise improvements to cyber security across their ICT systems. As a minimum, entities responded to current operational needs in delivering government services and in achieving compliance with government requirements. In general, the priority for additional cyber improvements was focused in delivering security controls for new ICT systems prior to deployment. There was limited evidence of assessment and formal planning to explain the level of priority given to other key enterprise assets (data and systems) and to high vulnerability systems.

4.24 In all three entities, cyber security investment initiatives were not addressing long-term strategic initiatives, instead being focused on short-term operational responses to identified cyber risks. Entities had approved annual capital and operations budgets for ICT systems. Entities did not have documented cyber initiatives beyond 2017–18 or a proposed investment budget for cyber security initiatives. However, at the time of the audit fieldwork in late 2017 the National Archives commenced an external review to inform its cyber investment initiatives in support of the Digital First program. Geoscience Australia also engaged an external reviewer to better understand its cyber resilience gap, including achieving compliance, and to inform its cyber investment initiatives beyond 2017–18.

Did entities have a cyber resilience culture?

The three entities were at different stages in embedding a cyber resilience culture. Treasury was aware of the importance of its sensitive data holdings and had ongoing activities to strengthen its cyber security approaches. National Archives had a number of longstanding practices and could have learnt more from looking outwardly to the cyber resilience practices of other entities. Geoscience Australia has traditionally had a culture of scientific independence that it had allowed to override cyber resilience considerations. All entities are aiming to better understand the shared attitudes, values and behaviours to make the most of ICT opportunities while effectively managing cyber risks.

4.25 The hallmarks of a cyber resilience culture are the set of shared attitudes, values and behaviours that characterise how an entity considers cyber risk in its day-to-day activities.[50] It requires more than compliance with government requirements and following a checklist of behaviours and practices that may improve an entity's cyber resilience; however being able to evidence those requirements, behaviours and practices can be considered an indicator of those attitudes and values being in place.

4.26 A cyber resilience culture promotes an open and proactive approach to managing cyber risk that considers both vulnerabilities and opportunity; and is one where cyber risk is appropriately identified, assessed, communicated and managed across all levels of the entity. Cyber resilient entities demonstrate a leadership culture and behaviours that prioritise cyber security and focus on it.

Progress towards a cyber resilience culture

4.27 All entities are on a journey to better understand the shared attitudes, values and behaviours expected from their leaders and management, staff and service providers, where a shared understanding of cyber risk leads to well informed decision making and investments to make the most of opportunities online. They each have different challenges in adopting and embedding a cyber resilience culture, reflecting their different circumstances.

- Treasury is aware of the importance of its sensitive data holdings and has ongoing activities to strengthen its cyber security, with cyber investments focused on critical services such as the Commonwealth Budget. There is entity-level oversight through governance committees and regular reporting of the cyber risks to the enterprise ICT systems. Security awareness and initiatives are noticeable behaviours amongst staff.
- National Archives had a number of longstanding practices and could have learnt more from looking outwardly to the cyber resilience practices of other entities.
- Geoscience Australia has had a culture of scientific independence that has been allowed to override cyber resilience considerations.[51] Insufficient cyber investments in past years reflect the entity's modest understanding of the critical role it plays in coordinating and reporting on national disasters. A new leadership team has escalated the assessment of

50 Borrowing from the hallmarks for a positive risk culture from the Commonwealth Risk Management Policy. Department of Finance, *Commonwealth Risk Management Policy*, 2014, available from <https://www.finance.gov.au/comcover/risk-management> [accessed 21 March 2018].

51 Geoscience Australia placed a high priority on allowing its staff to run applications on its systems in support of their scientific endeavours, with little priority given to the cyber security implications.

cyber risks and intended security posture; and is in the process of determining the investments required to achieve compliance.

4.28 The selected entities have implemented or are in the process of implementing a range of measures to build their cyber resilience culture to fit their business needs. Key measures included:

- an ICT program of work to maintain compliance and look beyond the Top Four mitigation strategies (Treasury and National Archives);
- a leadership culture and behaviours that prioritises cyber security, including appropriate investment (Treasury);
- key ICT operational staff with a sound understanding of the threats that may affect the enterprise ICT network, applications, databases and operating systems (all entities); and
- security awareness programs that address cyber security, including eLearning modules (all entities).

4.29 Further work is required by National Archives and Geoscience Australia to achieve compliance with the Top Four mitigation strategies. Until compliance is achieved—and a step closer to the goal of cyber resilience—it is inappropriate to assume that a positive cyber resilience culture is in place.

Behaviours and practices of cyber resilient organisations

4.30 As a result of this audit, the ANAO has outlined additional behaviours and practices of cyber resilient entities to assess against in future cyber security audits. Table 4.3 provides an updated checklist that may improve an entity's level of cyber resilience, many of which relate to risk management and governance arrangements. All entities are encouraged to assess the benefits of implementing these behaviours and practices in light of their own circumstances. In the absence of other guidance from the relevant entities, this will also form the basis of any future assessment of cyber resilient culture by the ANAO.

4.31 Attention should also be given to contracted ICT service providers and cloud computing services when assessing whether an entity has established key elements of a cyber resilient culture. Third party providers play a key role in the delivery of government services. Commonwealth entities need to consider the contributions and behaviours expected from third party providers in supporting the entity's cyber resilience culture, and reflect these in the service level agreements.

Table 4.3: Behaviours and practices that may improve the level of cyber resilience

Behaviours and practices assessed for the audited entities
Establish a business model and ICT governance that incorporates ICT security into strategy, planning and delivery of services.
Manage cyber risks systematically, including through assessments of the effectiveness of controls and security awareness training.
Develop and implement an integrated and documented architecture for data, systems and security controls.
Task enterprise-wide governance arrangements to have awareness of cyber vulnerabilities and threats.
Assign information security roles to relevant staff and communicate the responsibilities.
Develop the capabilities of ICT operational staff to ensure they understand the vulnerabilities and cyber threats to the system.
Adopt a risk-based approach to prioritise improvements to cyber security and to ensure higher vulnerabilities are addressed.
Additional behaviours and practices not assessed for the audited entities
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.
Identify and analyse security risks to their information and system, including documenting ICT assets requiring protection.
Develop an approach to verify the accuracy of self-assessments of compliance with mandatory cyber security requirements.
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.
Assign data ownership to key business areas, including the role to classify the data, and grant/revoke access to shared data by other entities.

Source: ANAO.

Grant Hehir
Auditor-General

Canberra ACT
28 June 2018

Appendices

Appendix 1 Responses from the selected entities

Formal responses received by the ANAO following circulation of the draft report are reproduced below.

Responses were received from:

- Department of the Treasury;
- National Archives of Australia;
- Geoscience Australia;
- Attorney-General's Department;
- Australian Signals Directorate; and
- Department of Home Affairs.

Australian Government

The Treasury

John A. Fraser
Secretary

27 April 2018

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

Dear Mr ~~Hehir~~ Grant

PROPOSED AUDIT REPORT ON CYBER RESILIENCE

Thank you for the opportunity to review and provide comment for the draft report on the Australian National Audit Office's performance audit of Cyber Resilience across the sampled agencies.

The Treasury agrees with the findings and all recommendations in the report. Benchmarking of Treasury's compliance against the Australian Signals Directorate's *Information Security Manual* will continue to be used to inform future cyber security strategies and policies.

I continue to affirm the importance of diligence and attentiveness to cyber security for all Treasury staff. The Treasury will continue to develop and implement robust cyber security strategies and policies to strengthen the security of Information and Communication Technology systems and mitigate the risk of cyber intrusion.

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

Kind regards

Yours sincerely

John A. Fraser

Langton Crescent, PARKES ACT 2600 • Telephone: 61 2 6263 3738 • Facsimile: 61 2 6263 3360

NATIONAL ARCHIVES OF AUSTRALIA

FROM THE OFFICE OF THE DIRECTOR-GENERAL

Our reference: 2018/1698

15/6/2018

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

Dear Grant

I write with respect to correspondence of 16 May 2018, inviting feedback on the Australian National Audit Office's (ANAO) Proposed Audit Report on Cyber Resilience. Thank you for the opportunity to comment.

We welcome the ANAO's report and recommendations on Archives' cyber resilience. I commend the Office's attention to and examination of this critical issue, which examined the preparedness of government agencies, including the Archives, to manage the associated cyber-risks to government data and information.

It is timely given the current work being undertaken by the Archives to develop a new whole-of-government digital information governance policy from 2020, providing the opportunity to draw on lessons learned through the audit.

Summary statement

The National Archives will develop a cyber resilience framework and a supporting plan to effectively implement the Essential Eight. It is intended the framework will underpin a secure, stable and contemporary ICT environment that supports the business of the National Archives. The activities to achieve the cyber maturity model for the National Archives will be prioritised by the National Archives Enterprise Board taking into consideration resourcing and whole-of-government posture for by cyber resilience.

Response to Recommendations

Recommendation 1

The National Archives agrees with the recommendation, and advises that a program of work will be planned in 2018-19, with monitoring of delivery to be managed internally and included in the Archives' mandatory compliance reporting. This program of work will include the activities to support application whitelisting and patching of operating systems.

Editorial matters

We have noted some minor editorial matters, which have been communicated directly to Lisa Rauter, Group Executive Director, Performance Audit Services Group.

PO Box 4924 Kingston ACT 2604 | 18 King George Terrace, Parkes ACT 2600
t (02) 6212 3600 | e archives@naa.gov.au naa.gov.au

Australian Government
National Archives of Australia

Shaun Rohrlach, Executive Officer for the National Archives, will be able to assist with coordinating further details on this matter. Phone: 02 6212 3990 or 0434 664 621.

Thank you again for the opportunity to comment.

Sincerely,

David Fricker

PO Box 4924 Kingston ACT 2604 | Queen Victoria Terrace, Parkes ACT 2600
t (02) 6212 3600 | e archives@naa.gov.au naa.gov.au

Australian Government
National Archives of Australia

Australian Government
Geoscience Australia

Cnr Jerrabomberra Avenue
and Hindmarsh Drive,
Symonston ACT 2609

GPO Box 378,
Canberra ACT 2601
Australia

+61 2 6249 9111
www.ga.gov.au

ABN 80 091 799 039

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

Dear Mr Hehir

Re: Proposed Audit Report on *Cyber Resilience*

Thank you for your letter of 16 May 2018 and for the opportunity to respond to the Australian National Audit Office's proposed report on *Cyber Resilience* in accordance with section 19 of *Auditor-General Act 1997*.

Geoscience Australia welcomes this report and agrees with the two recommendations. We agree that the report is an accurate assessment of our compliance at the time of the audit.

I would like to express my appreciation for the professional and collegiate approach taken by your audit team and their willingness to engage with us.

Geoscience Australia is committed to improving its security compliance and cyber resilience to a level appropriate for a government organisation that plays a role in providing scientific information and services to industry and the broader community.

We have already commenced actions to improve compliance to address the security issues identified including: the engagement of a senior consultant to advise on an overarching security framework; the establishment of a Security Working Group; and an action plan to address compliance with the Australian Signals Directorate's *Strategies to mitigate cyber security incidents*.

Attached are Geoscience Australia's summary response (annex A) and responses to recommendations (annex B).

Please contact Mr Trent Rawlings, Chief Operating Officer on (02) 6249 9411 if you require further information on our response.

Yours sincerely

Dr James Johnson
Chief Executive Officer
12 June 2018

Australian Government
Attorney-General's Department

Secretary

18/3514

7 June 2018

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

Dear Mr Hehir

Thank you for the opportunity to comment on the ANAO's proposed Cyber Resilience Audit Report. I acknowledge the recommendations about managing cyber risks and increasing cyber resilience across the Australian Government.

The department's response to the report's Recommendation 2 follows:

Recommendation No.2

In revising security reporting and cyber-related requirements under the Protective Security Policy Framework, the Attorney-General's Department, Department of Home Affairs and Australian Signals Directorate work together to improve compliance with the framework by:

(a) Providing adequate technical guidance to support entities to accurately self-assess compliance with the Top Four mitigation strategies and their underlying controls contained in the Information Security Manual

Agree. Proposed reforms to the Protective Security Policy Framework (PSPF), which are to take effect later this year, more clearly articulate the policy requirements for safeguarding information from cyber threats, as well as the links to underlying controls contained in the information security manual. The department notes the ANAO's paragraph 3.35 finding that '*it is important that the Australian Signals Directorate (ASD) develops such guidance (providing detailed control assessment test plans) to support the reporting changes underway*'; the department agrees to support ASD in this work.

(b) Developing a program for verifying entities' reported compliance with the mandatory cyber security requirements

Agree in principle. To support verification, the department's proposed reforms to the PSPF will introduce enhanced reporting obligations designed to provide greater assurance of the accuracy of entities' self-assessed reporting. For example, entities will be required to provide supporting

3-5 National Circuit, Barton ACT 2600 Telephone (02) 6141 6666 www.ag.gov.au ABN 92 661 124 436

evidence to demonstrate a cycle of security planning, monitoring and reporting each year, and explain how key security risks are managed.

Developing a verification program for cyber security is a matter for the Australian Cyber Security Centre. The department supports ASD and Department of Home Affairs considering possible further verification mechanisms and will provide assistance as appropriate.

(c) Increasing transparency and accountability about entities' compliance with those requirements

Agree. The department acknowledges the importance of improving transparency and accountability. To support this, the department agrees to publicly release the 2017-18 consolidated annual whole-of-government Protective Security Compliance Report (and future maturity reports).

The department is committed to achieving robust protective security across government, including on cyber security matters. The department, in consultation with entities across government, is currently leading significant reforms to protective security policy. Reforms to security reporting and cyber-related requirements are scheduled to commence in 2018.

The findings in this report will assist in the future delivery of effective protective security policy.

The contact officer for this matter is Emma Appleton who can be contacted on (02) 6141 2905.

Yours sincerely

Chris Moraitis PSM

Australian Government
Department of Defence

Director
Australian
Signals
Directorate

GPO Box 5076,
Kingston ACT 2604

Tel: +61 2 6255 0334
Fax: +61 2 6266 5731

File Ref: D18089405

Lisa Rauter
Group Executive Director
Performance Audit Services Group
Australian National Audit Office

Dear Lisa,

Please find below ASD's response to ANAO's proposed audit report on *Cyber Resilience* provided under section 19 of the *Auditor-General Act 1997*.

ASD agrees that the successful identification and management of cyber security risk is critical and your report demonstrates there is room for improvement.

ASD agrees with Recommendation 2. ASD acknowledges the inconsistent mapping between the 2017 *Australian Government Information Security Manual* and the *Essential Eight Maturity Model*. ASD is currently consulting on proposed changes to address this in the 2018 *Australian Government Information Security Manual* and continues to work with the Attorney-General's Department to ensure alignment with *Protective Security Policy Framework* reforms. While ASD provides cyber security advice to a variety of audiences, it remains the responsibility of Commonwealth entities to maintain a workforce of competent cyber security practitioners capable of assessing the effective implementation of security controls for their information and communication technology systems.

ASD agrees to continue working with the Attorney-General's Department and the Department of Home Affairs but notes that it is neither a regulatory body nor a compliance reporting agency. ASD works to provide better practice cyber security guidance to Commonwealth entities. ASD commends Commonwealth entities which achieve full compliance with mandatory requirement INFOSEC 4 from the *Protective Security Policy Framework* and also recognises the achievements of those making significant and sustained annual improvements to their cyber security posture.

ASD supports mature risk management frameworks for cyber security over compliance-based programs. Further, ASD encourages positive and sustained improvements to Commonwealth entities' cyber security posture over time. From experience we acknowledge that in some circumstances the application of all Top Four mitigation strategies may not be practicable, or introduces additional risks, and that other mitigating controls may achieve a similar overall outcome. ASD agrees to work with the Attorney-General's Department and

the Department of Home Affairs to assist both entities further their compliance measurements goals.

Yours sincerely,

Mike Burgess
Director
Australian Signals Directorate

13 June 2018

Australian Government
Department of Home Affairs

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

Dear Mr Hehir,

Thank you for the opportunity to provide comments on the Australian National Audit Office's (ANAO) report on *Cyber Resilience*.

The Department of Home Affairs (Home Affairs) has considered the relevant recommendation and has provided its response at Attachment A.

Home Affairs supports this recommendation. Home Affairs agrees there should be adequate technical guidance to support entities and a verification program for reported compliance. Home Affairs further supports the Australian National Audit Office's view that there should be increased transparency and accountability regarding entities' compliance.

If you have any questions in relation to the Home Affairs response, please contact David Norris, Assistant Secretary Audit and Assurance Branch on david.norris@homeaffairs.gov.au or (02) 6264 2022.

Yours sincerely

Mark Brown
A/g First Assistant Secretary
Integrity, Security & Assurance Division
27 June 2018

6 Chan Street Belconnen ACT 2617
PO Box 25 Belconnen ACT 2616 • Telephone: 02 6264 1111 • Fax: 02 6225 6970 • www.homeaffairs.gov.au

Appendix 2 Compliance grading scheme

1. In order to assess compliance consistently across the three entities, the ANAO applied a set of assessment criteria and developed a graphical key; a reporting convention similar to a 'traffic light' report. The keys are represented as either a Harvey Ball or cone. The key is outlined in Table A.1.

Table A.1: Key to grading scheme for assessing compliance with the Top Four mitigation strategies and ICT general controls

Grading scheme for mandatory ISM strategies	Grading scheme for ICT general controls
Controls not in place and no dispensation authorised by the Accountable Authority.	Control objectives not met.
Controls not in place but a dispensation is authorised by the Accountable Authority.	Identified controls not in place but compensating controls in place and observed.
Controls not in place but entity is actively implementing, with a minimum of design deliverables in evidence.	
Control in place and meeting control objectives.	Control objectives met.

Source: ANAO.

2. The selected entities were assessed on their:

- compliance with the Top Four mitigation strategies and related controls; and
- maturity to effectively manage logical access and change management as part of normal business processes (ICT general controls).

3. The ANAO's summary findings for each of the selected entities are reported in the context of a matrix, shown in Table A.1, which indicates entities' overall level of protection against internal and external threats as a consequence of steps taken to implement the Top Four mitigation strategies and ICT general controls. The matrix, which is referred to as the *Entity cyber security posture matrix*, indicates where entities are positioned in terms of cyber resilient zones: *vulnerable* zone; *externally resilient* zone; *internally resilient* zone, and *cyber resilient* zone.

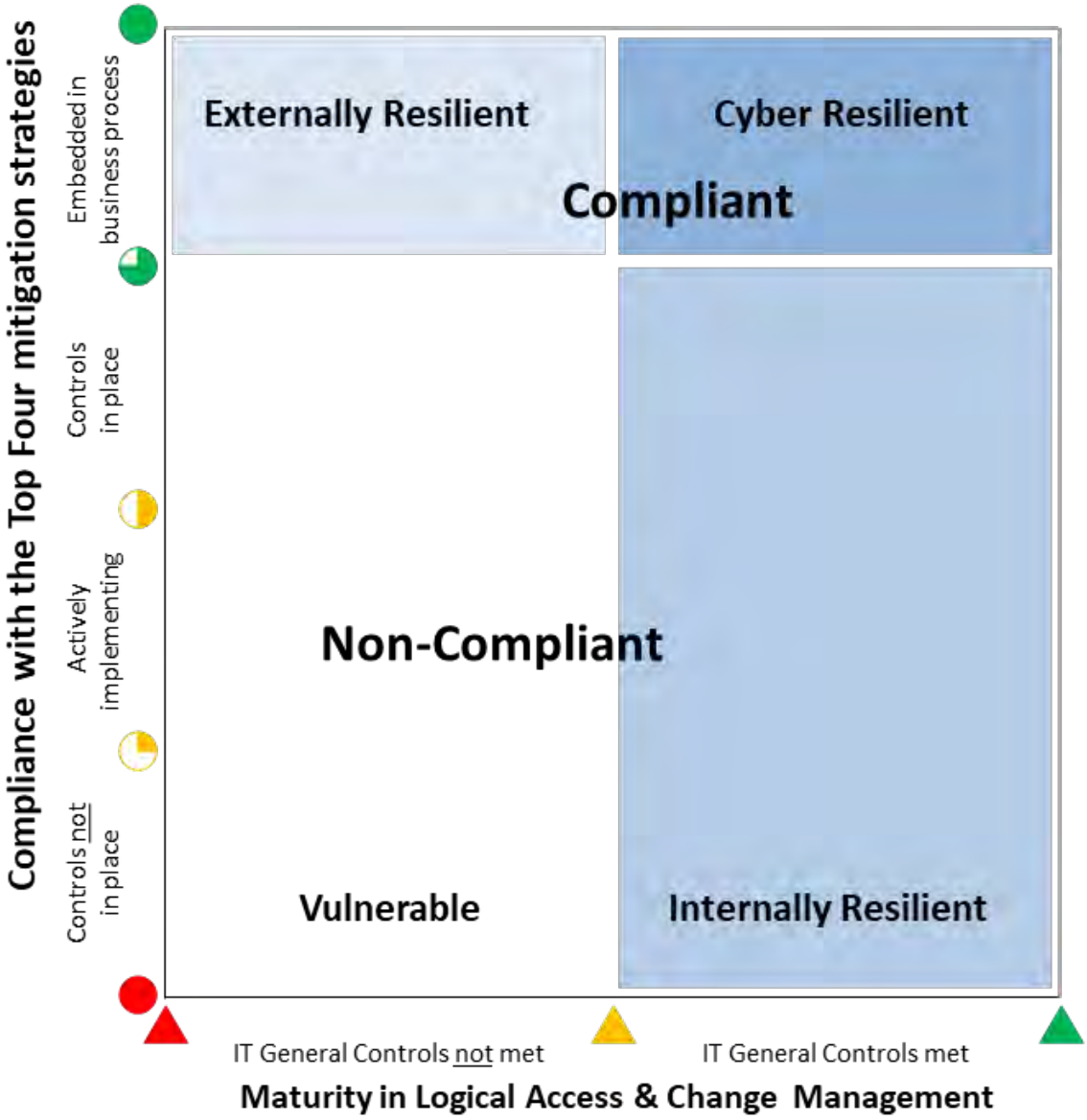
4. The zones are explained further in Table A.2 and illustrated in Figure A.1. An entity's position indicates its overall cyber resilience—in essence how well the entity is protecting its exposure to external vulnerabilities and intrusions, internal breaches and disclosures, and how well it is positioned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

Table A.2: Definitions of the Cyber Resilient zones

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

Source: ANAO.

Figure A.1: Entity cyber security posture matrix



Source: ANAO.

Appendix 3 The Essential Eight Maturity Model

		Maturity Level Three Fully aligned with intent of mitigation strategy
Mitigation strategies to prevent malware delivery and execution		
Application whitelisting	Workstations	Application whitelisting is implemented on all workstations Whitelisting of executables, software libraries, scripts and installers is enforced
	Server	Application whitelisting is implemented on all important servers (e.g. Active Directory, email servers and other servers handling user authentication) Whitelisting of executables, software libraries, scripts and installers is enforced
Patch applications	Workstations	Patches for extreme risk security vulnerabilities in Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers are applied and verified within 48 hours for all workstations Only vendor-supported versions of Adobe Flash, web browsers, Microsoft Office, Java and PDF viewers are used
	Server	Patches for extreme risk security vulnerabilities in web server software, other server applications that store important (sensitive or high-availability) data, and all other internet-accessible server applications are applied and verified within 48 hours for all servers Only vendor-supported versions web server software, server applications that store important data and other internet-accessible server applications are used
Configure Microsoft Office macro settings	Workstations	Only Microsoft Office macros in Trusted Locations with limited write access can execute Microsoft Office macros from the Internet are blocked Microsoft Office macro settings can't be changed by users
User application hardening	Workstations	Web browsers block or don't support Adobe Flash content Web browser Adobe Flash settings can't be changed by users Web browsers block web advertisements and Java from the Internet Flash and OLE functionality is disabled in Microsoft Office Unneeded features in Microsoft Office, web browsers and PDF viewers are disabled
Mitigation strategies to limit the extent of cyber security incidents		
Restrict administrative privileges	Workstations and servers	Requirements for privileged accounts are validated initially and on an annual or more frequent basis Duties-based restrictions on privileged accounts are applied All privileged accounts are blocked from reading emails and web browsing using technical controls

		Maturity Level Three Fully aligned with intent of mitigation strategy
Patch operating systems	Workstations	Patches for extreme risk security vulnerabilities in operating systems are applied and verified within 48 hours for all workstations Only vendor-supported operating system versions are used
	Servers	Patches for extreme risk security vulnerabilities in operating systems are applied and verified within 48 hours for all servers and network devices Only vendor-supported operating system versions are used
Multi-factor authentication	Workstations and servers	Multi-factor authentication is implemented for all users using remote access solutions (e.g. VPNs, remote desktops, corporate webmail) Multi-factor authentication is implemented for all users performing privileged actions Multi-factor authentication is implemented for all users accessing important (sensitive or high-availability) data repositories In addition to passphrases, only U2F security keys, physical OTP tokens, biometrics and/or smartcards are used for multi-factor authentication
Mitigation strategies to recover data and system availability		
Daily backups	Workstations and servers	Backups of important new/changed data, software and configuration settings are performed daily Backups are stored offline or otherwise disconnected from computers and networks, or online but in a non-rewritable and non-erasable manner Backups are stored for three months or greater Full recovery of backups has been tested Full recovery of backups has been tested after each fundamental IT infrastructure change Partial recovery of backups is tested on an annual or more frequent basis

Source: Australian Signals Directorate, *Essential Eight Maturity Model* [Internet], 2018. Available from <https://www.asd.gov.au/publications/protect/essential-eight-maturity-model.htm> [accessed 18 April 2018].

Appendix 4 Analysis of Top Four Mandatory Strategies to the Essential Eight Maturity Model—Patch Applications and Patch Operating Systems

Requirement of the Information Security Manual and *Protective Security Policy Framework*	Included in Maturity Model?	Rating?
High Assurance products must only be patched with ASD approved patches using methods and timeframes prescribed by ASD. [ISM 0300]	No	Not applicable
An approach for patching operating systems, applications, drivers and hardware devices that ensures the integrity and authenticity of patches, as well as the processes used to apply them, must be used. [ISM 0303]	No	Not applicable
Operating systems, applications and hardware devices that are no longer supported by their vendors must be updated to a vendor supported version or replaced with an alternative vendor supported version. [ISM 0304]	Yes	Maturity Level 1
Security vulnerabilities in operating systems, applications, drivers and hardware devices assessed as high risk must be patched or mitigated within two weeks of the security vulnerability being identified by vendors, independent 3rd parties, system owners or users. [ISM 0940]	No	Not applicable
A patch management strategy must be developed and implemented covering the patching of security vulnerabilities in operating systems, applications, drivers and hardware devices. [ISM 1143]	No	Not applicable
Security vulnerabilities in operating systems, applications, drivers and hardware devices assessed as extreme risk must be patched or mitigated within 48 hours of the security vulnerabilities being identified by vendors, independent 3rd parties, system owners or users. [ISM 1144]	Yes	Maturity Level 3

Requirement of the Information Security Manual and *Protective Security Policy Framework*	Included in Maturity Model?	Rating?
When patches are not available for security vulnerabilities, one or more of the following approaches must be implemented: • resolve the security vulnerability by either: – disabling the functionality associated with the security vulnerability; – asking the vendor for an alternative method of managing the security vulnerability; – moving to a different product with a more responsive vendor; and – engaging a software developer to resolve the security vulnerability. • prevent exploitation of the security vulnerability by either: – applying external input sanitisation (if an input triggers the exploit); – applying filtering or verification on output (if the exploit relates to an information disclosure); – applying additional access controls that prevent access to the security vulnerability; and – configuring firewall rules to limit access to the security vulnerability. • contain exploitation of the security vulnerability by either: – applying firewall rules limiting outward traffic that is likely in the event of an exploitation; – applying mandatory access control preventing the execution of exploitation code; and – setting file system permissions preventing exploitation code from being written to disk. • detect exploitation of the security vulnerability by either: – deploying an intrusion detection system; – monitoring logging alerts; and – using other mechanisms for the detection of exploits using the known security vulnerability. [ISM 0941]	No	Not applicable

Source: ANAO analysis.

Appendix 5 Findings from previous audits

Drawing on comparisons from past audits

1. ANAO Performance Audit Report No.50 2013–14 *Cyber Attacks: Securing Agencies' ICT Systems* (the first audit), was tabled in June 2014. In this audit, the ANAO examined seven entities'[52] compliance with the Top Four mitigation strategies and found that none of the seven entities were compliant with these strategies. The ANAO made three recommendations, which were agreed by all agencies (see later section in this Appendix). The entities accepted the audit findings and endorsed the three recommendations proposed by the ANAO.

2. The Joint Committee of Public Accounts and Audit (JCPAA) reviewed the first audit in October 2014.[53] Three of the seven audited entities—Australian Taxation Office, Department of Human Services and the then Australian Customs and Border Protection Service—appeared before the hearing to explain their plans and timeframes to achieve compliance. Each of the three entities gave assurance to the JCPAA that they would achieve compliance during 2016.

3. The JCPAA published its report in March 2015 and recommended that the seven entities achieve full compliance with the Top Four mitigation strategies as soon as possible. The JCPAA also recommended the Auditor-General consider a follow-up audit, as well as undertaking regular audits of Commonwealth entities' compliance with the Top Four mitigation strategies.

4. In 2015, the ANAO conducted a second performance audit to examine a further four government entities' compliance with the Top Four mitigation strategies. The four entities were: Australian Federal Police; Australian Transaction Reports and Analysis Centre; Department of Agriculture and Water Resources; and the Department of Industry, Innovation and Science. The ANAO Performance Audit Report No.37 2015–16 *Cyber Resilience* was tabled in May 2016. In this audit the ANAO found that two entities—Australian Transaction Reports and Analysis Centre, and the Department of Agriculture and Water Resources—were compliant with the Top Four mitigation strategies.[54] The other two entities were not compliant with these strategies.[55] The ANAO made three recommendations and all entities agreed with all recommendations.

5. In 2017, the ANAO conducted a follow-up audit of the cyber resilience of the three audited entities that appeared before the JCPAA hearing in October 2014. ANAO Performance Audit Report No.42 2016–17 *Cybersecurity Follow-up Audit* (the third audit) was tabled in March 2017. In this audit, the ANAO found that only the Department of Human Services was cyber resilient. To progress to being cyber resilient, the Australian Taxation Office and the Department of Immigration and

52 The seven entities were: Australian Bureau of Statistics; Australian Customs and Border Protection Service; Australian Financial Security Authority; Australian Taxation Office; Department of Foreign Affairs and Trade; Department of Human Services; and IP Australia.

53 Joint Committee of Public Accounts and Audit, The Parliament of the Commonwealth of Australia, *Report 447 EPBC Act, Cyber Security, Mail Screening, ABR and Helicopter Program: Review of Auditor-General Reports Nos 32–54 (2013–14)* (2016).

54 All four entities had self-reported compliance with the Information Security Manual to the ANAO at the start of audit fieldwork.

55 The non-compliant entities had initiatives underway but did not provide a timeframe when compliance would be achieved across their enterprise ICT systems.

Board Protection needed to improve their governance arrangements and prioritise cyber security.[56] The ANAO made two recommendations and all entities agreed with all recommendations.

Recommendations from previous audits

Audit Report No.50 2013–14 *Cyber Attacks: Securing Agencies' ICT Systems*

ANAO Recommendation No. 1

To achieve full compliance with the mandatory ISM strategies and related controls, the ANAO recommends that agencies:

(b) complete activities in train to implement the top four ISM controls across their ICT environments; and

(c) define pathways to further strengthen application whitelisting, security patching for applications and operating systems, and the management of privileged accounts.

Response from selected agencies: Agreed

ANAO Recommendation No. 2

To reduce the risk of cyber attacks to information stored on agency databases, the ANAO recommends that agencies strengthen logical access controls for privileged user accounts to the database by eliminating shared accounts, recording audit logs and monitoring account activities.

Response from selected agencies: Agreed

ANAO Recommendation No. 3

To strengthen their ICT security posture, the ANAO recommends that agencies:

(a) conduct annual threat assessments across the ICT systems, having regard to the Top 35 Mitigations Strategies—as proposed by the Australian Signals Directorate; and

(b) implement periodic assessment and review by the agency security executive of the overall ICT security posture.

Response from selected agencies: Agreed

Audit Report No.37 2015–16 *Cyber Resilience*

ANAO Recommendation No. 1

Entities establish processes to monitor patch levels across their enterprise ICT systems.

Response from selected entities: Agreed.

ANAO Recommendation No. 2

That entities:

(a) conduct periodic assessments on the effectiveness of IT security controls across their enterprise ICT systems;

(b) decide on the optimal and/or desired ICT security posture; and

(c) define strategies to achieve and maintain the desired ICT security posture.

56 Despite previously advising the JCPAA in October 2014 that full compliance would be achieved by December 2016, one non-compliant entity expected to achieve compliance by November 2017; the other entity could not provide a date when full compliance would be achieved.

Response from selected entities: Agreed.

ANAO Recommendation No. 3

That entities:

(a) capture and store audit logs for privileged user accounts; and

(b) actively monitor privileged user accounts for unauthorised access and inappropriate behaviour, preferably with the support of a security information and event management (SIEM) tool.

Response from selected entities: Agreed.

Audit Report No.42 2016–17 *Cybersecurity Follow-up Audit*

ANAO Recommendation No. 1

The ANAO recommends that entities periodically assess their cyber security activities to provide assurance that: they are accurately aligned with the outcomes of the Top Four mitigation strategies and entities' own ICT security objectives; and that they can report on them accurately. This applies regardless of whether cyber security activities are insourced or outsourced.

Response from selected entities: Agreed.

ANAO Recommendation No. 2

The ANAO recommends that entities improve their governance arrangements, by:

(a) asserting cyber security as a priority within the context of their entity-wide strategic objective;

(b) ensuring appropriate executive oversight of cyber security;

(c) implementing a collective approach to cyber security risk management; and

(d) conducting regular reviews and assessments of their governance arrangements to ensure its effectiveness.

Response from selected entities: Agreed.

Appendix 6 Top 4 Mitigation Strategies and other applicable controls

1. The *Information Security Manual* includes a section on Information Technology Security that sets out the specific controls for which compliance is required by the *Protective Security Policy Framework.* A table summarising these controls is reproduced below:

Mitigation strategy	Chapter and section of *Information Security Manual*	Control numbers
Application whitelisting	Software Security – Standard Operating Environments	0843, 0846, 0955, 1391, 1392
Patch applications	Software Security – Software Patching	0300, 0303, 0304, 0940, 0941, 1143, 1144
Patch operating systems	Software Security – Software Patching	0300, 0303, 0304, 0940, 0941, 1143, 1144
Restrict administrative privileges	Access Control-Privileged Access	0445, 0985, 1175
	Personnel Security for Systems – Authorisations, Security Clearances and Briefings	0405

Source: Australian Signals Directorate, *Information Security Manual*, [Internet], 2017, p. 122, available from <https://www.asd.gov.au/publications/Information_Security_Manual_2017_Controls.pdf>, [accessed 18 April 2018].

2. The same section also identifies other applicable controls which, while not mandatory are 'best practice for a Top 4 implementation and complement the mandatory controls listed above.'[57]

Mitigation strategy	Chapter and section of *Information Security Manual*	Control numbers
Application whitelisting	Software Security – Standard Operating Environments	0845, 0957, 1413
Patch applications	Software Security – Software Patching	0297, 0298, 1467
Patch operating systems	Software Security – Software Patching	0297, 0298, 1407
Restrict administrative privileges	Access Control – Privileged Access	0446, 0447, 0448
	Personnel Security for Systems – Authorisations, Security Clearances and Briefings	0407
Configure Microsoft Office macro settings Software Security – Standard Operating Environments 1411	N/A	N/A

57 Australian Signals Directorate, *Information Security Manual*, [Internet], 2017, p. 11, available from <https://www.asd.gov.au/publications/Information_Security_Manual_2017_Controls.pdf>, [accessed 18 April 2018].

Mitigation strategy	Chapter and section of *Information Security Manual*	Control numbers
User application hardening	Software Security – Standard Operating Environments	1409, 1411–1412
Multi-factor authentication	Access Control – Identification, Authentication and Authorisation, Cross Domain Security – Gateways, Secure Administration – Secure Administration	0974, 1039, 1173, 1357, 1384, 1401
Daily backups	Information Security Documentation – Business Continuity and Disaster Recovery Plans	0118, 0119

Source: Australian Signals Directorate, *Information Security Manual*, [Internet], 2017, p. 123, available from <https://www.asd.gov.au/publications/Information_Security_Manual_2017_Controls.pdf>, [accessed 18 April 2018].