Joint Committee of Public Accounts and Audit

Cyber Resilience: Inquiry into Auditor-General Reports 1 & 13 (2019–20)

Submission by the Australian National Audit Office

2 June 2020

1. Cyber resilience is the ability to continue providing services while deterring and responding to cyber intrusions. Cyber resilience reduces the likelihood of successful cyber intrusions. To become cyber resilient, an entity needs to first establish effective information and communication technology (ICT) general controls. Effective ICT general controls provide a stable and reliable foundation upon which other processes and controls can be built. An entity also needs to effectively implement the Top Four cyber security risk mitigation strategies as outlined in the Information Security Manual.[1] 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 adapt to disruptions caused by cyber security incidents while maintaining continuous business operations.

2. Starting in 2013–14, the Auditor-General has tabled an ongoing series of performance audits in the Parliament on Australian Government entities' cyber security and cyber resilience. Four of the audits examined cyber security and cyber resilience of non-corporate Commonwealth entities while one examined Government Business Enterprises and corporate Commonwealth entities:

   - Auditor-General Report No.50 of 2013–14 *Cyber Attacks: Securing Agencies' ICT Systems*;
   - Auditor-General Report No.37 of 2015–16 *Cyber Resilience*;
   - Auditor-General Report No.42 of 2016–17 *Cybersecurity Follow-up Audit*;
   - Auditor-General Report No.53 of 2017–18 *Cyber Resilience*; and
   - Auditor-General Report No.1 of 2019–20 *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities*.

3. The five performance audits found that Australian Government entities' compliance with mandatory requirements of the Protective Security Policy Framework (PSPF) for information security remained low, and that the regulatory framework had not driven sufficient improvement

[1] The Top Four mandatory strategies to mitigate cyber security risks, as outlined in the Information Security Manual, are: application whitelisting; patching applications; restricting administrative privileges; and patching operating systems. These strategies are mandatory for non-corporate Commonwealth entities.

in cyber security. The audits identified that only six of 17 entities (35 per cent) were compliant with the requirements for implementing all the Top Four cyber security risk mitigation strategies.

4. As a continuation of the cyber security and cyber resilience performance audit series, the ANAO is currently conducting an audit on *Cyber Security Strategies of Non-Corporate Commonwealth entities*. This audit examines the effectiveness of cyber security risk mitigation strategies implemented by selected non-corporate Commonwealth entities to meet mandatory requirements under the PSPF, and the support provided by the responsible cyber policy entities. The audit is due to table in the Parliament in late 2020.

5. As requested by the Committee on 19 May 2020, the ANAO has provided in this submission the common themes on cyber security and cyber resilience that were identified in previous Auditor-General reports based on key findings from those audits.

6. In July 2018, the ANAO published an edition of Audit Insights that covered the key learnings from Auditor-General reports tabled up to June 2018 relating to cyber resilience. This submission builds on those insights with findings from the 2019–20 *Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities* audit and the *Interim Report on Key Financial Controls of Major Entities* which was published in May 2020.

Key ANAO audit findings and themes

Cyber security and cyber resilience of non-corporate Commonwealth entities

7. Between 2013–14 and 2017–18, the ANAO conducted four performance audits to assess the cyber security and cyber resilience of 14 non-corporate Commonwealth entities. The audits identified that only four entities (29 per cent) had complied with mandatory PSPF requirements for information security (Top Four mitigation strategies).

8. The ANAO found that while efforts have been made to achieve compliance, there were:

   - low levels of compliance for application whitelisting, particularly for servers (higher levels of compliance for desktops);
   - variable levels of compliance for security patching of applications and operating systems (lower for operating systems); and
   - shortcomings in a number of entities with respect to restricting administrative privileges.

9. The four performance audits also examined whether the non-corporate Commonwealth entities subject to audit coverage were cyber resilient. The ANAO found that only four (29 per cent) of the 14 entities were cyber resilient. These were the same four entities that the ANAO found to be compliant with all the mandatory requirements for implementing the Top Four mitigation strategies.

10. The ANAO audit coverage has identified that the low levels of compliance with mandatory cyber security requirements and cyber resilience were driven by shortcomings in the entities' governance arrangements, including:

    - a lack of effective cyber security strategy;
    - entities not adopting a risk–based approach in their prioritisation of cyber security improvements; and

- cyber security investments being focussed on short-term operational needs rather than long-term strategic objectives.

11. In June 2018 the ANAO published, as part of Auditor-General Report No.53 of 2017–18 *Cyber Resilience*, a list of behaviours and practices that may assist agencies to build a strong cyber resilience culture. The following table outlines the list of behaviours and practices that contribute to entities having a strong cyber resilience culture.

Table 1: Behaviours and practices that may improve the level of cyber resilience

Governance and risk management
1. Establish a business model and ICT governance that incorporates ICT security into strategy, planning and delivery of services.
2. Manage cyber risks systematically, including through assessments of the effectiveness of controls and security awareness training.
3. Task enterprise-wide governance arrangements to have awareness of cyber vulnerabilities and threats.
4. Adopt a risk-based approach to prioritise improvements to cyber security and to ensure higher vulnerabilities are addressed.
Roles and responsibilities
5. Assign information security roles to relevant staff and communicate the responsibilities.
6. Develop the capabilities of ICT operational staff to ensure they understand the vulnerabilities and cyber threats to the system.
7. 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.
8. Embed security awareness as part of the enterprise culture, including expected behaviours in the event of a cyber incident.
9. Assign data ownership to key business areas, including the role to classify the data, and grant or revoke access to shared data by other entities.
Technical support
10. Develop and implement an integrated and documented architecture for data, systems and security controls.
11. Identify and analyse security risks to their information and system, including documenting ICT assets requiring protection.
12. 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.
Monitoring compliance
13. Develop an approach to verify the accuracy of self-assessments of compliance with mandatory cyber security requirements.

12. The ANAO noted that cyber resilient 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 and embedded it the culture of the organisation. These entities understood the risk profile across their enterprise ICT systems, and managed those risks systematically, including 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.

13. Entities with a cyber resilience culture have a set of shared attitudes, values and behaviours that characterise how an entity considers cyber risk in its day-to-day activities. Cyber resilience requires more than compliance with government requirements and following a checklist of behaviours and practices that may improve an entity's cyber resilience. 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 security and cyber resilience of Government Business Enterprises and corporate Commonwealth entities

14. As noted in the Auditor-General's opening statement to the Committee at the hearing on 19 May 2020, Auditor-General Report No.1 of 2019–20 found that:

    - the three entities incorporated mitigation strategies and controls from the Information Security Manual in their cyber security risk management frameworks, despite not being mandated to do so. Two of the entities (Reserve Bank of Australia and Australian Postal Corporation) went further and incorporated aspects of recognised national and international cyber security frameworks applicable to their industry or regulatory environments; and

    - two of the entities (Reserve Bank and ASC Pty Ltd) had implemented controls for the Top Four and the other Essential Eight mitigation strategies in the Information Security Manual.[2] The third entity had not fully implemented controls for either the Top Four or the four non-mandatory mitigation strategies in the Essential Eight.

15. In addition, Auditor-General Report No.1 of 2019–20 found that all three entities had implemented mitigation strategies beyond the requirements of the Essential Eight, such as the Reserve Bank using machine learning and analytics to detect cyber threats.

16. The three entities were at different stages in embedding a cyber resilience culture. The ANAO found that the Reserve Bank had embedded all 13 behaviours and practices (as outlined in Table 1 of this submission) that contributed to a strong cyber resilience culture within its organisation. ASC is developing a cyber resilience culture and Australia Post is working towards embedding a cyber resilience culture within its organisation.

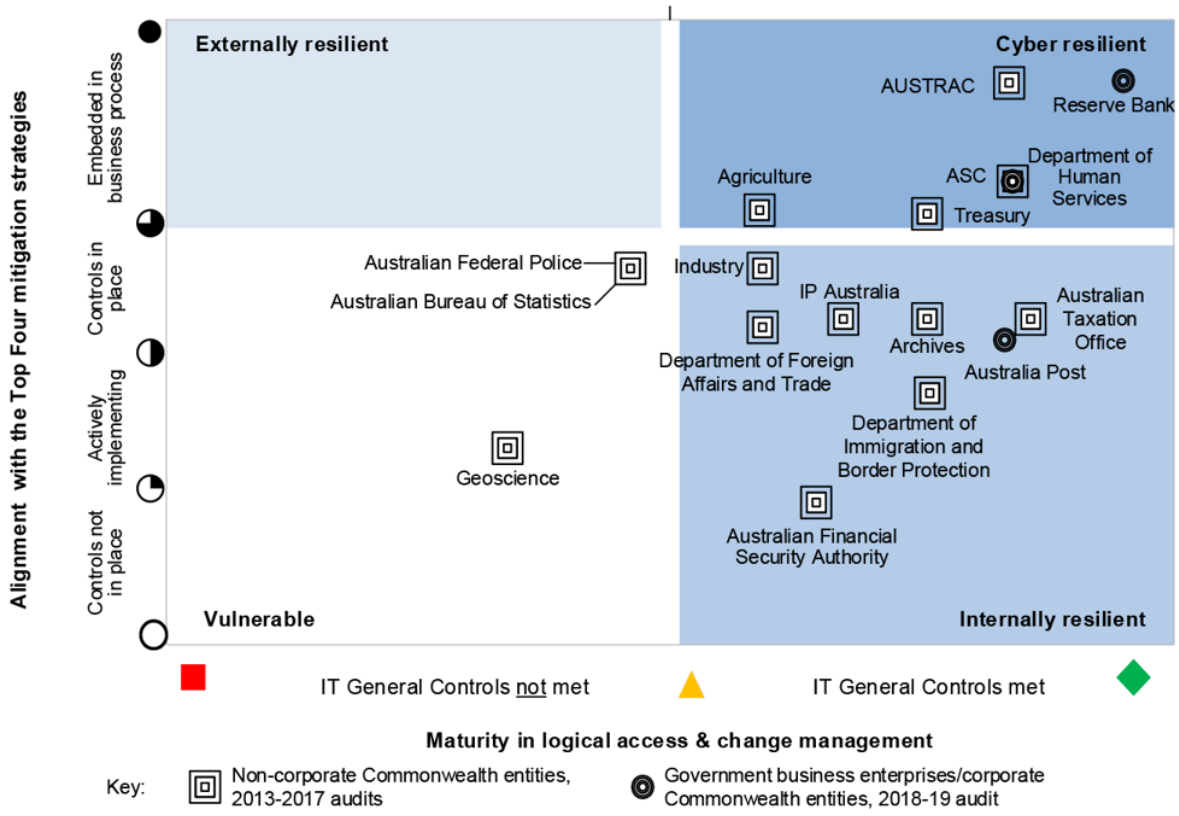
17. The ANAO found two of the three entities (Reserve Bank and ASC) to be cyber resilient. These two entities had implemented the Top Four cyber security risk mitigation strategies and had established effective ICT general controls (refer paragraph 1 of this submission). The Reserve Bank

[2] The four non-mandatory mitigation strategies of the Essential Eight are: disabling untrusted Microsoft Office macros; hardening the configuration of user applications; applying multi-factor authentication; and managing daily backups.

and ASC had high levels of cyber resilience compared to the other 15 entities under the ANAO audit coverage over the past six years.

18. Auditor-General Report No.1 of 2019–20 presented the ANAO assessments of cyber resilience for all 17 entities audited over the past six years in Figure 1.

Figure 1: ANAO assessments of entities' cyber resilience



Note: The position of each entity in the diagram is the position that was allocated at the time of the latest ANAO audit assessment.

19. Given the small number of Government Business Enterprises and corporate Commonwealth entities that the ANAO had assessed (three), it is not possible to draw conclusions as to the relative level of cyber resilience of corporate compared to non-corporate Commonwealth entities.

Interim Report on Key Financial Controls of Major Entities 2019–20

20. The Auditor-General's *Interim Report on Key Financial Controls of Major Entities* was published in May 2020 and includes an assessment of entities' key internal controls that supported the preparation of the 2019–20 financial statements of 24 entities. The report also includes a review of the self-assessed level of compliance with mandatory cyber security controls of 18 entities[3] against the PSPF Policy 10 (INFOSEC-10) requirements. The review was undertaken to confirm

[3] Due to the timing of the interim audit work, two entities were excluded from the ANAO analysis. These entities were: Future Fund Management Agency and the Board of Guardians, and the Australian Office of Financial Management. Four additional entities — Australian Postal Corporation, National Disability Insurance Agency, NBN Co Limited, Reserve Bank of Australia — were excluded as they are corporate Commonwealth entities or Commonwealth companies that are not required to report on compliance with the PSPF.

the accuracy of reporting and identify cyber security risks that may impact on the preparation of financial statements.

21. The ANAO found that the maturity levels for the majority of the entities reviewed were below the required PSPF Policy 10 maturity level of 'Managing'.[4] Of the 18 entities assessed, only one was rated as achieving a 'Managing' maturity level across all mandatory controls. The ANAO found that 76 per cent of controls reviewed were at an 'Ad hoc' or 'Developing' maturity level.[5] The regulatory framework and self-assessments to date have not driven the achievement of the standard of cyber security required by Government policy.

Oversight and support for the implementation of cyber security requirements

22. As noted at paragraph 4, the ANAO is currently conducting a performance audit on *Cyber Security Strategies of Non-Corporate Commonwealth entities*. One of the criteria in the audit examines whether the three entities responsible for cyber policy (the Australian Signals Directorate, the Attorney-General's Department and the Department of Home Affairs) have worked together to support accurate self-assessment and reporting by non-corporate Commonwealth entities, and to improve those entities' implementation of cyber security requirements under the PSPF. This criteria assesses the implementation of Recommendation 2 from Auditor-General Report No.53 of 2017–18 *Cyber Resilience*.

[4] From 2018–19, entities report on their PSPF compliance using a maturity model to assess the maturity of their protective security practices. For PSPF Policy 10, entities' self-assessment of their implementation level of the Top Four mitigation strategies will inform their overall maturity level. The maturity levels are: Ad hoc; Developing; Managing; and Embedded. A maturity level of 'Managing' is achieved where all Top Four mitigation strategies have been fully implemented.

[5] According to the Attorney-General's Department, an 'Ad hoc' maturity level is achieved where the Top Four mitigation strategies have been partially implemented. A 'Developing' maturity level is achieved where an entity has implemented the majority of the Top Four mitigation strategies.