Review of Cyber Security

Australian National Audit Office

Report by the Independent Auditor

December 2017

ISBN 978-1-76033-310-2 (Print)
ISBN 978-1-76033-311-9 (Online)

4 December 2017

Dear Mr President
Dear Mr Speaker

I have undertaken a performance audit of the Australian National Audit Office, in accordance with the authority contained in section 45 of the *Auditor-General Act 1997*.

I present the report of this audit to the Parliament. The report is titled *Australian National Audit Office Performance Audit: Review of Cyber Security*.

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

Yours sincerely

Peter van Dongen
Independent Auditor
Appointed under Section 41 of
The Auditor-General Act 1997

Contents

Abbreviations

AASG	Assurance Audit Services Group
ACSC	Australian Cyber Security Centre
the Act	*Auditor-General Act 1997*
AGD	Attorney-General's Department
ANAO	Australian National Audit Office
ASA	Agency Security Adviser
ASAE	Australian Auditing and Assurance Standard
ASD	Australian Signals Directorate
AAWP	Annual Audit Work Program
CAB	Change Advisory Board
CERT	Computer Emergency Response Team
CISO	Chief Information Security Officer
CMB	Corporate Management Branch
EBOM	Executive Board of Management
EL	Executive Level
ICT	Information and Communication Technology
ISM	Information Security Manual
IT	Information Technology
ITSA	Information Technology Security Adviser
ITSC	Information Technology Security Committee
JCPAA	Joint Committee of Public Accounts and Audit
PASG	Performance Audit Services Group
PSPF	Protective Security Policy Framework
SES	Senior Executive Staff
SNARE	System Intrusion Analysis and Reporting Environment
Top Four	ASD's Top Four mandatory cyber security mitigations

1. Executive summary

Background to the performance audit

1.1 The performance audit topic of cyber security was selected following discussions with the Joint Committee of Public Accounts and Audit (JCPAA), consideration of previous performance and internal audit reports, the current Australian National Audit Office (ANAO) Internal Audit Plan and external factors currently impacting the ANAO.

Audit objective

1.2 The objective of this performance audit was to assess the effectiveness of ANAO's internal processes at minimising unauthorised exposure of their client's electronic data and the effectiveness of the methodology, technology and capability of ANAO in delivering the cyber security reviews of other Australian Government entities.

Audit approach

1.3 In conducting this performance audit, the following approach was undertaken:

- I reviewed ANAO's processes in place to minimise unauthorised exposure or loss of client data. This included:
  - Obtaining an understanding of the ANAO's current data holdings and the process for identifying critical and sensitive datasets;
  - Obtaining an understanding of the ANAO's current security strategy and governance model;
  - Evaluating the effectiveness of the ANAO's 2016 Protective Security Policy Framework (PSPF1) self-assessment, including consideration of the critical and sensitive datasets;
  - Evaluating the effectiveness of the ANAO's last self-assessment against the Australian Signals Directorate (ASD)'s Top 37 cyber mitigation strategies (henceforth the Top 37), including application of the ASD's Top Four cyber security mitigations (henceforth the Top Four): application whitelisting, patching applications, patching operating systems and minimising administrative privileges;
  - Evaluating whether the status of the ANAO's security strategy is being effectively reported to and reviewed by the appropriate governance bodies, including how the ANAO is meeting the external reporting requirements of the Attorney General's Department (AGD) and the ASD; and

1 Available at www.protectivesecurity.gov.au.

  - Reviewing the effectiveness of the ANAO's cyber awareness training through review of the training and awareness materials and attendance records for staff and contractors.

- I assessed the effectiveness of the methodology, technology and capability of the ANAO to deliver cyber security reviews through its own program of work. This included:
  - Reviewing the methodology for delivering cyber security reviews across Australian Government entities, including the sampling of entities, testing methodology and the reliance on other parties; and
  - Assessing the strategy (including supporting personnel and technology) for the 2016-2017 cyber security review.

Conclusion

1.4 The ANAO has a risk based approach for dealing with sensitive and classified information. Most importantly, the approach implemented for handling the most sensitive information accessed by ANAO staff is to only access the data directly on the Australian Government entity's network. Even though this approach significantly reduces the inherent cyber security risk to client's classified data, ANAO still needs to develop a formal data governance framework and implement appropriate security controls to protect personal and sensitive data that ANAO holds on its network.

1.5 Although there is no documented cyber security strategy to guide decisions being made by the Change Advisory Board (CAB) and IT Security Committee (ITSC), cyber security is considered in key IT decisions made by the ANAO. The Executive Board of Management (EBOM) receive IT security reporting; however, without a formal cyber security strategy that defines the long-term security objectives for the ANAO, the EBOM cannot fully assess the effectiveness of the CAB and ITSC. The ANAO IT Strategic Plan has not defined the current state or desired future state of ANAO organisational security controls. Once a strategy has been documented, linkages to other key strategies including at least, the corporate strategy, IT strategy, business continuity and disaster recovery strategies is critical. The EBOM sponsorship of these strategies will ensure that the appropriate priority and funding is allocated for the identified security initiatives.

1.6 ANAO have implemented 26 of the Top 37 recommended by ASD[2]. Even though none of the Top Four had been implemented effectively at the time of reporting to the AGD, ANAO reported full compliance for INFOSEC4[3] in their 2016 PSPF reporting.

1.7 Prior to the ANAO's self-reporting of 2016 PSPF compliance, a 2015 internal audit identified weaknesses in the Top Four that were not remediated or accepted as risks within the ANAO's risk appetite. Like the Top Four, the majority of ANAO's cyber security controls are currently preventative controls, intended to prevent cyber security attacks from breaching the ANAO IT environment. These controls are operated by service providers and the ANAO does not effectively monitor the implementation of these controls, or assess the risk of known deficiencies[4].

2 https://www.asd.gov.au/infosec/top-mitigations/mitigations-2017-details.htm .

3 The ASD INFOSEC4 obligation states that Australian Government entities must document and implement operational procedures and measures to ensure information, systems development and systems operations are designed and managed in accordance with security, privacy, legal and regulatory obligations under which the entity operates.

4 This is consistent with key findings from the ANAO's performance audits on the effectiveness of other Australian Government entities' cyber security controls.

1.8 The ANAO currently has limited detective controls in place that would identify the unauthorised exposure of client data by either a trusted insider or an external attacker that breaches the network perimeter. The ANAO has an incident management process to manage identified security incidents and has the capability to deal with common security incidents, although would require external support to deal with a complex security incident, which is commensurate with other Australian Government entities of a similar size. The current incident management process does not define the criteria for when and how the ANAO should engage with the ASD to seek assistance in responding and recovering from an incident, although there are clear criteria for which type of incidents must be reported to the ASD.

1.9 The Auditor-General identifies and selects performance audits through the Annual Audit Work Program (AAWP). This program is developed after the assessment of potential benefits, level of public and parliamentary interest and risk to reputation and service delivery[5]. As per the *Auditor-General Act 1997*, the final decision on which audits comprise the AAWP is at the sole discretion of the Auditor-General.

1.10 The ANAO has contributed to an improved awareness of cyber security risks and key mitigating controls across Government since 2014, although has only reviewed eleven different Australian Government entities over this period of time. In April 2013, AGD made amendments to the PSPF mandating the Top Four to be enacted with immediate effect[6]. As a result, in 2014, the ANAO undertook a review of seven Australian Government entities to assess their compliance with the Top Four. This was further supported through the related *Cyber Resilience* (2015-16 No. 37) and *Cybersecurity Follow-up Audit report* (2016-17 No. 42) in 2017. Through these reports, ANAO has played an important role in supporting the enforcement of the Top Four.

1.11 Cyber security is one of the emerging risks across Federal Government, highlighted by the release of Australia's first Cyber Security Strategy[7] in 2016. As part of the 2016/17 AAWP, the ANAO conducted 1 out of a total of 57 performance audits with a cyber security focus. This audit was a follow up review on a previous ANAO cyber security related performance audit, and as a result, the scope included only 3 out of more than 200 Australian Government entities.

1.12 The ANAO does not currently have the internal capacity or capability to deliver an expanded scope of cyber security audits, but does have access to external resources (including consultants and contractors) as required.

5 ANAO Annual Audit Work Program 2017-18, https://www.anao.gov.au/work-program/introduction-2017.

6 ANAO Audit Report No.50 2013–14 Cyber Attacks: Securing Agencies' ICT Systems, https://www.anao.gov.au/work/performance-audit/cyber-attacks-securing-agencies-ict-systems.

7 Issued by the Prime Minister and accessible at https://cybersecuritystrategy.pmc.gov.au/.

Summary of key recommendations

1.13 For ANAO's own IT environment:

- Enhance the data governance framework and further drive the prioritisation of required security controls by improving the communications channels/processes from audit teams to the Chief Information Officer (CIO) and Information Technology Security Adviser (ITSA). This communication is to identify the most sensitive stakeholder data held within the ANAO IT environment which requires protection.
- Create a cyber security strategy to prioritise the required security improvements to further strengthen the security controls of the ANAO IT environment. These controls should include:
  - the Essential Eight[8] (incorporating the Top Four) cyber security mitigations recommended by the ASD (henceforth the Essential Eight);
  - specific controls with a high cost-benefit value to the ANAO's IT environment; and
  - key detective security controls e.g. implementing more network and host based monitoring.
- Document and maintain a security risk assessment that includes a register of ANAO's IT security controls, additional risk treatments required or accepted risks under the ANAO's risk management framework.
- Define a process that identifies when and how to engage with the ASD when responding[9] to a security incident, and if ASD support was not available in a timely manner due to other ASD priorities, how the security incident would be handled by the ANAO.
- Improve the monitoring of security controls by ensuring segregation of duties between the staff responsible for operating key security controls and the ITSA that is monitoring and reporting on them.
- Improve the cyber security reporting to ensure that senior management are aware of the progress against the security plan, the current effectiveness of key controls, and any prioritisation decisions required of senior management.
- Continue with the current Information Security Registered Assessors Program (IRAP) assessment in progress to validate the effectiveness of current security policies and controls across the IT environment and inform the prioritisation of remediation of key control deficiencies.

8 JCPAA Report 467 on Cybersecurity Compliance issued in October 2017 recommended that Australian Government mandate the Essential Eight for all Public Governance, Performance and Accountability Act 2013 entities, by June 2018. This represents two changes: increasing the mandatory controls for non-corporate Australian Government entities from the Top Four to the Essential Eight and making the Essential Eight mandatory for corporate Australian Government entities where they are currently only recommended.

9 The process for mandatory reporting of security incidents to ASD is documented. This recommendation relates to the expectations of support (from internal staff, service providers and potentially ASD) to respond to an on-going security incident.

1.14 For the ANAO's cyber security performance audits of other Australian Government entities:

- Seek more detailed information from AGD, ASD[10] and in the future, the Australian Security and Intelligence Organisation (ASIO) and the Office of the Australian Information Commissioner (OAIC), so as to inform greater analysis of cyber security risks. This will enable the Auditor General to exercise his discretion in determining the AAWP (including the number of cyber security audits and the number of entities and controls in scope).
- Ensure the resources (developed internally or sourced externally) are available to undertake any future expanded scope of cyber security audits[11] and a potentially larger program of IT performance audits. This would require increases in and access to:
  - experience and qualifications in more specialist cyber security capabilities including; security operations centres (SOC), security information and event management (SIEM) systems, network security and cloud security;
  - capacity to conduct IT performance audits, which may include an increased scope of IT general controls testing of systems other than financial and human resources systems; and
  - experience and qualifications in complementary skillsets such as data privacy, data governance and IT (including cloud) architectures.

Overall ANAO response

Agreed. The ANAO takes cyber security very seriously - both as an organisation and as an Audit Institution. This is reflected in the Auditor-General's ongoing allocation of resources to cyber security in the Annual Audit Work Program. The ANAO's 2017-18 Corporate Plan also ensures an ongoing focus on cyber security through the organisational priority - *Advanced ICT strategies and systems*. As the report notes, where issues have been identified the ANAO has taken prompt action to address them. The ANAO agrees with the recommendations contained in the report and is well advanced in addressing each recommendation.

10 All Australian Government entities are required to report cyber security incidents to the ASD and all non-corporate Australian Government entities are required to report their self-assessment on PSPF compliance, which includes assessing compliance with the ISM and the Top Four. JCPAA Report 467 has recommended that all PGPA entities report their compliance with the Essential Eight, which will provide additional information on corporate Australian Government entities that is not currently reported to AGD.

11 This could include auditing the effectiveness of cyber security mitigations recommended by the ASD but not mandated by AGD through the PSPF, or could include an audit of the effectiveness of the self-assessment and reporting regime under the PSPF as recommended by the JCPAA in Report 467 into Cybersecurity Compliance.

2. Background – This Performance Audit

The Independent Auditor

2.1 Mr Peter van Dongen, the Independent Auditor for the ANAO, has undertaken this performance audit. Mr van Dongen is also a Managing Partner of PricewaterhouseCoopers (PwC) Australia.

2.2 Pursuant to Schedule 2[12] of the Auditor-General Act 1997, the Independent Auditor is appointed by the Governor-General for a term of three years and not more than five years. Mr van Dongen was appointed as the Independent Auditor of the ANAO on 12 June 2014.

Audit objective

2.3 The objective of this performance audit is to assess the effectiveness of ANAO's internal processes at minimising unauthorised exposure of their client's electronic data and the effectiveness methodology, technology and capability of the ANAO in delivering cyber security reviews of other Australian Government entities.

Audit scope

2.4 The scope of this performance audit was developed after consultation with key stakeholders and focused on the following areas:

- ANAO's processes to minimise unauthorised exposure or loss of client data.
- Effectiveness of the methodology, technology and capability of the ANAO to deliver cyber security reviews through its own program of work.

2.5 The following areas are out of scope for this performance audit:

- Testing of any controls outside of the ANAO's control.
- Detailed assessment or re-performance of controls assessed by the ANAO as part of its three previous performance audits on cyber security and cyber resilience.

Audit methodology and approach

2.6 This performance audit was conducted in accordance with Australian Auditing and Assurance Standard ASAE 3500 Performance Engagements[13]. The planning process identified that the scope for this performance audit would focus on the assessment of ANAO's internal process that appropriately minimise the exposure of their clients' electronic data. This performance audit would also assess the effectiveness in delivering cyber security reviews of other Australian Government entities.

12 Schedule 2, Section 1 of the *Auditor-General Act 1997*.

13 *Standard on Assurance Engagements* ASAE 3500 *Performance Engagements* (July 2008) issued by the Auditing and Assurance Standards Board.

2.7 In conducting this review, the following steps were undertaken:

- Reviewed ANAO's processes to minimise unauthorised exposure or loss of client data, by:
  - Obtaining an understanding of the ANAO's current data holdings and the process for identifying critical and sensitive datasets;
  - Obtaining an understanding of the ANAO's current security strategy and governance model;
  - Evaluating the effectiveness of ANAO's 2016 PSPF self-assessment (dated August 2016), including consideration of the critical and sensitive datasets;
  - Evaluating the effectiveness of ANAO's 2016 self-assessment against the Top 37, including application of the Top Four: application whitelisting, patching applications, patching operating systems and minimising administrative privileges;
  - Evaluating whether the status of the ANAO's security strategy is being effectively reported to and reviewed by the appropriate governance bodies, including how the ANAO is meeting the external reporting requirements of the AGD and the ASD; and
  - Reviewing the effectiveness of ANAO's cyber awareness training through review of the training and awareness materials and attendance records for staff and contractors.
- Determined the effectiveness of the methodology, technology and capability of the ANAO to deliver cyber security reviews through its own program of work, by:
  - Reviewing the methodology for delivering cyber security reviews across Australian Government entities, including the sampling of entities, testing methodology and the reliance on other parties.
  - Assessing the strategy (including supporting personnel and technology) for the 2016-2017 cyber security review.

2.8 During the course of the performance audit, interviews were held with the:

- Assurance Audit Services Group (AASG) and Performance Audit Services Group (PASG) Group Executive Directors;
- Executive Directors of the AASG, PASG, and Corporate Management Branch (CMB);
- Executive Level and APS staff through focus group sessions[14]; and
- Representatives from the ANAO's key service providers.

2.9 The focus of the interviews and review of key documentation were to gain an understanding of the existing processes that are in place at ANAO to mitigate the risks associated with the exposure of clients' electronic data.

14 Four separate focus group sessions were conducted in July 2015 with APS level staff from each of AASG, PASG, PSB and CMB.

3. Audit observations and recommendations

Context

3.1 The ANAO 2016-20 Corporate Plan is the primary strategic planning document that outlines the purpose, strategic directions and key organisational capabilities. The plan also sets out four key focus areas providing a framework for achieving its purpose, which are to deliver:

- annual financial statements audits of Australian Government entities;
- assurance reviews of Australian Government entities;
- performance audits of Australian Government programs and entities; and
- sharing information and expertise, including the publication of better practice guides.

3.2 In delivering these services, ANAO accesses or makes copies of client information of varying classification levels. ANAO must ensure that appropriate levels of technical and non-technical controls are in place to protect client information against cyber threats. These controls should be designed to protect client information under a number of scenarios, including:

- Electronic records stored on the ANAO network being accessed by ANAO staff or contractors without authorisation;
- Electronic records stored on the ANAO network being accessed by an external attacker without authorisation;
- Electronic records copied from the ANAO network on to servers managed by third parties (including cloud providers);
- Electronic records copied from the ANAO network onto physical media by ANAO staff or contractors;
- Electronic records accessed from an ANAO stand-alone laptop; and
- Electronic records accessed from another Australian Government entity's network using an ANAO staff or contractor's logon.

3.3 The ANAO 2016-20 Corporate Plan provides direction to ANAO in delivering evidence based audit services and independent reporting to Parliament, the Executive and the public, with the result of improving public sector performance.

3.4 The ANAO Strategic Planning Framework facilitates the ANAO's governance and business planning and includes key elements like risk management via the Corporate Plan, forward Audit Program, Audit Committees and EBOM.

Positive observations

3.5 The ANAO's strategic decision to analyse the most sensitive information on the auditee IT environments, thereby not copying the data to the ANAO network or devices significantly reduces the inherent cyber security risks associated with maintaining copies of national security information (above Protected) and large sensitive datasets on the ANAO IT environment.

3.6 There is a strong security culture engrained in ANAO audit and operational staff who are collecting, maintaining and responsible for securing sensitive information. This was demonstrated by management's prioritisation of remediation activities in responding to governance and control deficiencies identified during the audit.

Audit observations: Practices that could be improved

Finding 1 – IT Security of the ANAO's IT environment

Context

3.7 Information security strategies are fundamental to how organisations shape their approach to cyber security. An information security strategy should document the strategic direction and long-term objectives for cyber security that have been derived through consideration of the cyber security risks faced by an organisation in addition to its business conditions (such as its business objectives, financial limitations, legislative obligations and risk appetite). A clear and endorsed cyber security strategy should define the current state of security, the desired state, and how the desired state will be achieved (through people, processes and technology) and be reviewed semi-annually or annually to ensure alignment to business objectives.

3.8 With the rapidly growing cyber security threat landscape, it is necessary for organisations to understand their information and data risks and protect their critical information assets – including private, sensitive and security classified data – from malicious adversaries. Cyber security threats come in many forms, including malware and phishing attacks, identity theft and ransomware. In order to prevent attackers and mitigate vulnerabilities, multiple security controls may be required at various locations and be coordinated as part of a layered defence-in-depth approach. The cyber security strategy should identify and prioritise the data security controls required to ensure that the sensitive information is only disclosed to authorised parties (confidentiality), prevent unauthorised modification of data (integrity) and help guarantee the data can be accessed by authorised parties when requested (availability).

3.9 As per the Australian Cyber Security Centre (ACSC) cyber threat report, the number of cybersecurity incidents rose 260 per cent from 2011 to 2014 i.e. 313 cyber incidents in 2011 to 1,131 in 2014[15]. Since then the extent of cyber threats have grown exponentially. From July 2015 to June 2016, Computer Emergency Response Team (CERT) Australia responded to 14,804 security incidents affecting Australian businesses and ASD responded to 1095 cyber security incidents on government systems from January 2015 to June 2016[16].

3.10 The ANAO has two service groups; Assurance Audit Services Group (AASG) and Performance Audit Services Group (PASG). AASG provides independent assurance and reviews on

15 Threat Report 2015 – Australian Cyber Security Centre, https://www.acsc.gov.au/publications/ACSC_Threat_Report_2015.pdf.

16 Threat Report 2016 – Australian Cyber Security Centre, https://acsc.gov.au/publications/ACSC_Threat_Report_2016.pdf.

the financial statements and financial administration, and PASG conducts performance audits, over Australian Government entities. While delivering these services, ANAO accesses sensitive personal information and nationally security classified information ranging from Unclassified up to Top Secret, but only stores information on its corporate network rated up to and including Protected.

3.11 Within the ANAO, the Professional Services and Relationships Group (PSRG) and Corporate Management Branch (CMB) provide technical and administrative support to the services groups and the Auditor-General. ANAO host two systems, eHive and Teammate, to store and process client data. These two systems are able to store information classified up to and including Protected.

3.12 The most sensitive data accessed by ANAO staff resides on the IT networks of the Australian Government entity who own the data and should not be stored or copied on any ANAO IT assets. The cyber security controls protecting this information are the responsibility of each Australian Government entity and not the ANAO. This approach reduces the inherent risk of cyber security attack for the ANAO.

3.13 The ANAO does store a significant volume of Protected and Unclassified Dissemination Limiting Marker (DLM) information, so there is still reliance on the cyber security controls protecting the ANAO network and its data from cyber security threats.

3.14 The ANAO 2017-18 Corporate Plan provides guidance to ANAO's operating environment and outlines the key components such as performance, capabilities, governance and risk management. This document also has linkages to various audit manuals, policies, procedures and methodologies which provides guidance to staff for conducting audits. The 'Capability' section of the ANAO 2017-18 Corporate Plan indicates the development of advanced IT strategies and systems to deliver a flexible, responsive and connected environment.

3.15 The ANAO has an IT Security Committee (ITSC) and has outlined the roles and responsibilities for performing security related activities, as recommended by the PSPF. This committee includes representation from ANAO's main branches and key IT decisions are supported by existing formal governance processes such as CAB and EBOM.

3.16 The ANAO IT Strategy Plan includes the prioritised IT initiatives for the next 3 years, of which, the majority will contribute to the cyber security of the IT environment. There is no formal security strategy that documents the current state of security controls or the desired state. Other than the ANAO IT Strategy Plan, there is no other strategic document that prioritises future security initiatives.

3.17 ANAO previously had the CIO also act as the ITSA. In October 2016, a dedicated ITSA was appointed to report directly to the Senior Executive Director, Corporate Management Branch. As a result there is now segregation of duties between the operation and monitoring of security controls; although the ITSA remains a part-time role and continues to be prioritised around other IT activities. This additional role represents an increase in the ANAO's investment in security operations, where on-going funding will require continued prioritisation by management for it to remain effective.

Observations

3.18 At the time of this audit, ANAO were not as strong as those recommended by the ASD or the AGD to protect data from unauthorised access or disclosure. Such shortcomings could mean that the ANAO are likely to be more vulnerable to cyber-attacks than the Australian Government entities owning the data, where those Australian Government entities meet the recommendations of ASD and AGD.

3.19 Throughout the audit process, once brought to their attention, management reacted quickly to prioritise remediation of deficient security controls mitigating key risks.

3.20 The ANAO's security governance did not identify that the ANAO was non-compliant with the Top Four in August 2016, which resulted in incorrectly reporting compliance with these controls. Security governance has since been strengthened to include an independent assessment of controls on a regular basis.

3.21 The ANAO has current staff and service providers that can respond to security incidents, but a complex security incident would likely require additional specialist support. The ANAO's incident management framework does not clearly define the scenarios when it would rely on the support of the ASD, and if support was unavailable due to other ASD priorities, how ANAO would respond to the security incident.

3.22 There is no formal security roadmap that defines the prioritised security improvements and the level of funding required to implement them.

Risk exposure

3.23 The ANAO are likely to be more vulnerable to cyber-attacks than the Australian Government entities owning each dataset, where those Australian Government entities meet the recommendations of ASD and AGD. The cyber security audits conducted by the ANAO over the past four years have identified similar weaknesses in the equivalent security controls at eight of the eleven audited Australian Government entities. As these Australian Government entities improve their security controls, the ANAO should improve their own commensurately.

Recommendations

3.24 Enhance the data governance framework and further drive the prioritisation of required security controls by improving the communications channels/processes from audit teams to the CIO and ITSA. This communication is to identify the most sensitive stakeholder data held within the ANAO IT environment which requires protection.

3.25 Create a cyber security strategy to prioritise the required security improvements to further strengthen the security controls of the ANAO IT environment. These controls should include:

- the Essential Eight[17] (incorporating the Top Four) cyber security mitigations recommended by the ASD (henceforth the Essential Eight);
- specific controls with a high cost-benefit value to the ANAO's IT environment; and
- key detective security controls e.g. implementing more network and host based monitoring.

3.26 Document and maintain a security risk assessment that includes a register of ANAO's IT security controls, additional risk treatments required or accepted risks under the ANAO's risk management framework.

3.27 Define a process that identifies when and how to engage with the ASD when responding[18] to a security incident, and if ASD support was not available in a timely manner due to other ASD priorities, how the security incident would be handled by the ANAO.

3.28 Improve the monitoring of security controls by ensuring segregation of duties between the staff responsible for operating key security controls and the ITSA that is monitoring and reporting on them.

3.29 Improve the cyber security reporting to ensure that senior management are aware of the progress against the security plan, the current effectiveness of key controls, and any prioritisation decisions required of senior management.

3.30 Continue with the current IRAP assessment in progress to validate the effectiveness of current security policies and controls across the IT environment and inform the prioritisation of remediation of key control deficiencies.

ANAO response

Agreed**.** The findings and recommendations from this report will assist ANAO to enhance its cyber security approach.

17 JCPAA Report 467 on Cybersecurity Compliance issued in October 2017 recommended that Australian Government mandate the Essential Eight for all Public Governance, Performance and Accountability Act 2013 entities, by June 2018. This represents two changes: increasing the mandatory controls for non-corporate Australian Government entities from the Top Four to the Essential Eight and making the Essential Eight mandatory for corporate Australian Government entities where they are currently only recommended.

18 The process for mandatory reporting of security incidents to ASD is documented. This recommendation relates to the expectations of support (from internal staff, service providers and potentially ASD) to respond to an on-going security incident.

- The ANAO has a sound approach to managing client data that is collected as part of an audit. This approach is guided by the Audit Manuals that prescribe processes based on policies, audit standards and audit methodology. In addition, the ANAO has identified opportunities across its strategic governance framework to enhance the corporate processes that support audit teams to collect, handle and store audit evidence. The ANAO will include standing agenda items at the IT Strategic Committee that require Senior Audit managers to report on ongoing conformance with corporate policies.

- The ANAO agrees to develop a cyber security strategy to complement its existing suite of governance documents including the ANAO Corporate Plan, IT security policy and ANAO strategic risk framework. The ANAO notes that the ISM and PSPF do not require an organisation to develop a security strategy. The ANAO has regard to both the ISM and PSPF in developing its approach to security and has existing policies that cover information security, personal security and physical security. The ANAO agrees to include in the cyber security strategy its approach regarding the Essential Eight controls particularly those controls that have a high cost-benefit value to the ANAO's IT environment.

- The ANAO has implemented a risk register that identifies PSPF requirements and the ANAO's treatment and risk assessment of those controls. The register is monitored through a sound governance framework which includes the monthly ANAO Security Committee meeting, the IT Strategic Committee which is a sub-committee of the ANAO's Executive Board of Management.

- The ANAO has updated the Incident Response Plan as part of the IRAP assessment to include more direction on when to contact ASD. The ANAO notes that its Incident Response Plan contained guidance on when to contact ASD prior to the recent update. The ANAO will review its documents to provide additional guidance on how to manage an incident where ASD was not available.

- The ANAO recognised the importance of segregating the duties of the ITSA in October 2016, splitting the role from the CIO and appointing a dedicated ITSA at that time. The ANAO notes the Independent Auditor's observation that the ITSA has other duties and will monitor the workload to ensure IT security functions continue as a priority.

- ANAO has improved reporting mechanisms through its governance framework to ensure that cyber security is prioritised, monitored and reviewed. The development of the cyber security strategy will assist the ANAO in the management and reporting of progress to senior management.

- The ANAO is nearing completion of the IRAP assessment. The ANAO continues to implement improvements and recommendations from the assessment.

Finding 2 – ANAO Performance Audits of other Australian Government entities' cyber security controls

Context

3.31 The ANAO is a specialist public sector practice that provides assurance and performance audit services across the federal government. The ANAO 2016-20 Corporate Plan outlines the ANAO's purpose, the detailed plan to achieve this purpose and the strategic focus.

3.32 The ANAO performance audits are conducted to independently evaluate the administration of entities or their programs, functions, policies and procedures to assess if they are achieving economy, efficiency and effectiveness while utilising available resources[19]. The ANAO performance audit program plays a vital role in improving administration and management practices of Australian Government entities.

3.33 The ANAO has developed a performance audit guide which provides detailed process for their staff to conduct performance audits. The performance audit topics are identified and selected during the AAWP planning process. Selection is based on the potential benefit, level of public and parliamentary interest and risk to reputation and service delivery. An appropriate consultative processes is also considered across the government entities and priorities are determined by the Auditor General with advice from the JCPAA.

3.34 Over the past four years, the ANAO has audited a sample of critical security controls recommended by the ASD at eleven[20] Australian Government entities. The ANAO leveraged advice from the ASD to prioritise the controls reviewed, which were those made mandatory by the PSPF and are all preventative controls. The ANAO chose the Australian Government entities to audit and the audit scope for those entities.

3.35 JCPAA Report 467 recommends "that the Australian Government mandate the Australian Signals Directorate's Essential Eight cybersecurity strategies for all Public Governance, Performance and Accountability Act 2013 entities, by June 2018" and that "the Auditor-General consider conducting an audit of the effectiveness of the self-assessment and reporting regime under the Protected Security Policy Framework".

Observations

3.36 The ANAO audit approach focused on the IT general controls protecting the financial management and human resource management information systems of the selected Australian Government entities, and a sample of technical security controls that protect their respective corporate networks and other business systems. While the approach considered the overarching control framework (on gateways and networks) the approach did not consider the specific data privacy controls or IT general controls that protect non-financial critical business systems. While the ANAO

19 http://www.isaca.org/chapters10/Lusaka/NewsandAnnouncements/Documents/Pefromance-Auditing.pdf.

20 Australian Government entities included three of the four entities with the largest IT environments (Department of Human Services, Australian Taxation Office and the Department of Immigration and Border Protection), as well as the Australian Bureau of Statistics, the Australian Financial Securities Authority, the Department of Foreign Affairs and Trade, IP Australia, the Australian Federal Police, the Australian Transaction Reports and Analysis Centre, the Department of Agriculture and Water Resources and the Department of Industry, Innovation and Science.

reports do state in the body of the report that these specific systems[21] were sampled, this focus is not easily identifiable in the executive summary.

3.37 The overall recommendations of the three cyber security audits are enterprise-wide recommendations that have been extrapolated based on the assessment of controls in place protecting only the examined corporate networks, financial management and human resource management information systems. It is possible that other control deficiencies, with different root causes, would have been identified if the ANAO's audit sampling had been expanded to validate the operating effectiveness of security controls applied to other critical business systems.

3.38 As emerging cyber security threats have continued to evolve, the number of entities sampled for each audit has not increased[22], and the scope of controls assessed by the ANAO at each entity has remained consistent with the Top Four. The ANAO is currently planning the fourth cyber security audit and is considering the selection of three entities and expanding the scope of controls at each entity to the Essential Eight. Currently there are no plans to specifically assess other critical security controls in the Top 37, or complementary frameworks like data governance, as they are not mandated by the PSPF.

3.39 The ANAO cyber security audits in aggregate have found that a significantly lower percentage of audited entities are compliant with the Top Four (27%), compared with all entities that self-report compliance (65%) to AGD. JCPAA Report 467 noted that this was "despite the fact that the Top Four mitigation strategies represent the minimum requirement for entities" and that most entities should be doing more. Across the ANAO cyber security audits, seven recommendations have been made, all of which were targeted at the eleven entities audited. No recommendations have been made about the effectiveness of the PSPF in managing cyber security risks across other Australian Government entities, and if the ANAO audit results are indicative of the discrepancy between self-assessed compliance levels and actual compliance levels, many more Australian Government entities may not be fully aware of the effectiveness of their Top Four controls and therefore, the current level of cyber security risk they are accepting.

3.40 The National Institute of Standards and Technology (NIST) Cybersecurity Framework[23] has five functions: Identify, Protect, Detect, Respond and Recover. The Top 37 categorises their controls in a similar manner, covering all functions other than Identify. The Top Four are all within the Protect function, and the Essential Eight currently include Protect, Detect, Respond and Recover controls. All five functions are fundamental to minimising unauthorised data exposure, and different technical expertise are required to assess the operating effectiveness of each function. The audit teams that conducted the cyber security audits had relevant qualifications and experience to assess the Protect related controls. When the scope of controls expands to include Detect, Respond and Recover related controls, more technical cyber security expertise will be required by the ANAO.

Risk exposure

3.41 The ANAO could have provided significantly more comfort to Parliament over the increasing cyber security risks facing Australian Government entities by investing more of its budget in performing cyber security related audits.

21 Systems included two corporate applications: financial management information systems and human resource management information systems, as well as three desktop applications: Microsoft Excel, Adobe Reader and Java.

22 Seven entities were sampled in 2013-2014, three entities in 2015-2016 and three of the original seven entities were revisited in 2016–2017.

23 NIST Framework for Improving Critical Infrastructure Cybersecurity Draft Version 1.1.

Recommendations

3.42 Seek more detailed information from AGD, ASD[24] and in the future, the Australian Security and Intelligence Organisation (ASIO) and the Office of the Australian Information Commissioner (OAIC), so as to inform greater analysis of cyber security risks. This will enable the Auditor General to exercise his discretion in determining the AAWP (including the number of cyber security audits and the number of entities and controls in scope).

3.43 Ensure the resources (developed internally or sourced externally) are available to undertake any future expanded scope of cyber security audits[25] and a potentially larger program of IT performance audits. This would require increases in:

- experience and qualifications in more specialist cyber security capabilities including; security operations centres (SOC), security information and event management (SIEM) systems, network security and cloud security;
- capacity to conduct IT performance audits, which may include an increased scope of IT general controls testing of systems other than financial and human resources systems; and
- experience and qualifications in complementary skillsets such as data privacy, data governance and IT (including cloud) architectures.

ANAO response

Agreed. The ANAO audit approach for cyber security audits focussed on four security layers: gateway, network, application and desktop. This approach provided a basis for comparison across the often quite disparate entities included in the audits. Application level controls were assessed for the financial management and human resource management information systems, and for common desktop productivity applications which are often targeted in a cyber security intrusion. While it is correct that the selection of different applications may have identified different strengths and weaknesses at the application layer, the controls at the gateway, network and desktop level were not influenced by the selection of applications for review.

When developing our Annual Audit Work Program the ANAO will consult with relevant entities. The Joint Committee of Public Accounts and Audit has requested that the ANAO conduct cyber security performance audits in corporate Commonwealth entities and government business enterprises. An audit is included in the Auditor-General's current annual audit work program. ANAO capability to undertake cyber audits will be assessed as part of the development of the Annual Audit Work program and scoping of individual audits, including sourcing and developing the appropriate skills.

24 All Australian Government entities are required to report cyber security incidents to the ASD and all non-corporate Australian Government entities are required to report their self-assessment on PSPF compliance, which includes assessing compliance with the ISM and the Top Four. JCPAA Report 467 has recommended that all PGPA entities report their compliance with the Essential Eight, which will provide additional information on corporate Australian Government entities that is not currently reported to AGD.

25 This could include auditing the effectiveness of cyber security mitigations recommended by the ASD but not mandated by AGD through the PSPF, or could include an audit of the effectiveness of the self-assessment and reporting regime under the PSPF as recommended by the JCPAA in Report 467 into Cybersecurity Compliance.

Appendices

Appendix 1: Top Four cyber security mitigation strategies

Detailed information on the ANAO's current implementation of the Top Four was provided directly[26] to ANAO management.

26 Based on the sensitivity of the data, it was agreed not to include in the public report.

Appendix 2: Top 37 cyber security mitigation strategies

Detailed information on the ANAO's current implementation of the Top 37 was provided directly[27] to ANAO management.

27 Based on the sensitivity of the data, it was agreed not to include in the public report.

Appendix 3: Organisational risks

This review was related to the following strategic and operational risks for the ANAO:

Strategic risk 3 – The ANAO does not keep pace, in a contestable environment, with reliable, efficient and professional business practices.

- Operational risk 8 – The ANAO does not support business requirements and audit program delivery through IT BAU services.
- Operational risk 10 – The ANAO's security regime is inadequate to provide the required level of protection to ANAO assets.
- Operational risk 11 – The ANAO does not properly protect large aggregate electronic data sets and files obtained to support audit work.
- Operational risk 12 – The ANAO is unable to continue business operations in the event of an emergency.

Strategic risk 4 – The ANAO does not achieve the quality standards required to support its work.

- Operational risk 13 – Forming of an incorrect Audit opinion/ conclusion.

Strategic risk 5 – The ANAO duplicates effort by not effectively leveraging the data and information it collects.

- Operational risk 17 – The ANAO does not engage and manage capability effectively to meet business needs.
- Operational risk 18 – The ANAO does not assess, monitor and invest in emerging technologies or update and maintain technology supporting audits.

Appendix 4: Key ANAO documents and external references

The following key documentation were reviewed as part of this performance audit:

Key ANAO related documents[28]

- ANAO 2016-20 Corporate Plan
- ANAO Risk Management Framework
- ANAO Strategic Planning Framework
- ANAO Performance Audit Guide
- ANAO Audit Work Program Planning
- ANAO Patching Implementation Plan v1.3
- ANAO User New Admin Account Creation
- ANAO Identity Access Management Guidance
- ANAO Secure Room Guidelines v1.1
- ANAO IT Committee Reports
- ANAO Risk Register - Dec 2016
- ANAO (CO-13072) ICT Network IRAP Report 1 0 - Document requirements
- ANAO (CO-13072) ISM 2013 August Release Checklist version 1.0D for auditors
- ANAO 2015-16 PSPF Compliance Overview
- ANAO PSPF Compliance Report 2016 - Letter to Chris Moraitis
- ANAO PSPF Compliance Report 2016 - Letter to the Prime Minister
- ANAO Protective Security Risk Review v4.2 2017 (Final)
- Draft ANAO Security Plan v2.7
- AppLocker Policy Management v1.2
- Internal Audit of IT Security May 2015 Report
- ITSC February 2017 Update on IRAP and ASD Top Four
- Release SOE Application Patches v1
- SNARE Monthly Report - Feb 2017
- FW PSPF compliance report for ANAO for year ending 30 June 2016 DLM For-Official-Use-Only email
- Issues Log at 9 March 2017

28 All key ANAO related documents were sourced during the fieldwork phase of this performance audit. (April to July 2017).

- Cyber Security Follow-up Audit – Artefact List
- Guideline - change management test
- Testing template for ITGC Change Management CTP
- Testing template Linux UNIX server hardening patching test scripts
- Testing template Patching CTP (Template ISM2015)
- Testing template Patching Test Process Diagram
- Testing template Privileged User Access Testing Template v02
- Testing template Whitelisting CTP (Template based on ISM 2015)

External references

- Auditor-General Act 1997.
- ASD Guidelines for Top Four Mandatory Security Mitigation Strategies
- ASD Guidelines for Top 37 Strategies to Mitigate Cyber Security Incidents Assessment
- AGD Guidelines for Protective Security Policy Framework
- Australian Government Information Security Manual