OFFICIAL

Joint Committee of Public Accounts and Audit

Answers to Questions on Notice

Inquiry into Commonwealth Financial Statements 2021–22

Department/Agency: Australian National Audit Office
Topic: Protective Security Policy Framework (PSPF)
Date of Hearing: 19 May 2023
Type of question: Written
Date set by the committee for the return of answer: Friday 2 June 2023

Number of pages: 1

Question 1: How does the ANAO assess entities' cybersecurity measures?

Answer:

1. The ANAO assesses an entity's cyber security measures by determining which measures are relevant to the audit, whether for Financial Statements audit or as part of a cyber performance audit. The ANAO assesses the entity's PSPF maturity self-assessments, strategies, plans, processes and system configurations against the Protective Security Policy Framework (PSPF), Essential Eight Maturity Model (Essential Eight) and Information Security Manual (ISM). The approach includes:
    - review of PSPF self-assessments for Policy 10: *Safeguarding information from cyber threats,* or other PSPF policies as relevant;
    - system testing and technical assessment of the relevant cyber security controls implemented. This is based on the PSPF and the ACSC's prescribed guidance within the Essential Eight and ISM[1];
    - examine relevant documentation relating to their cyber security strategies and activities, including: security risk assessments undertaken, project plans for cyber security improvement programs established, and records of minutes for any governance forums established for cyber security;
    - meetings with relevant staff.

[1] For entities not required to implement the PSPF, the framework used by the entity is considered and where there is no other framework in place, the PSPF, Essential 8 and ISM are used as a better practice framework to assess against.

OFFICIAL

Joint Committee of Public Accounts and Audit

Answers to Questions on Notice

Inquiry into Commonwealth Financial Statements 2021–22

Department/Agency: Australian National Audit Office
Topic: Protective Security Policy Framework (PSPF)
Date of Hearing: 19 May 2023
Type of question: Written
Date set by the committee for the return of answer: Friday 2 June 2023

Number of pages: 2

Question:
According to the ANAO, what are the reoccurring challenges that government entities face in implementing effective controls for the timely removal of user access to government systems and data?

Answer:

1. Some of the challenges identified through our audit work in implementing effective controls for timely removal of user access to government systems and data are:
    - poor management of contractor access;
    - mitigating controls, such as monitoring of user activities and periodic validation of user access, are either not established or are not operating effectively;
    - delays in notifications of the requirement to remove the access, such as when personnel change duties, leave the organisation or a contract is ceased;
    - lack of clarity around the roles and responsibilities between IT and business areas resulting in controls not being consistently performed; and
    - entities not monitoring whether notifications are actioned by the Shared Services entities providing user access management services. [1]
2. The ANAO has also identified the following issues that increase the risk of entities not appropriately removing user access:
    - a lack of policies encompassing user access removal or that define the timeframe access should be removed from systems following a user's departure from the entity;
    - the HR system reflects an incorrect separation date if entities cannot backdate termination/cessation records; and
    - a lack of robust mitigating controls to detect unauthorised and inappropriate user access to reduce the risks associated with failures in processes and controls for removing access.[2]

[1] Auditor-General Report No.14 2021-22 *Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2021*, paragraphs 2.44-2.48
[2] Auditor-General Report No.8 2022-23 *Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2022*, paragraphs 2.101-2.104

OFFICIAL

Joint Committee of Public Accounts and Audit

Answers to Questions on Notice

Inquiry into Commonwealth Financial Statements 2021–22

Department/Agency: Australian National Audit Office
Topic: Protective Security Policy Framework (PSPF)
Date of Hearing: 19 May 2023
Type of question: Written
Date set by the committee for the return of answer: Friday 2 June 2023

Number of pages: 2

Question:
3. Can the ANAO provide an outline of its findings?

4. Can you provide examples of moderate and minor findings related to IT security management and user access?

7. Apart from user access termination controls, what other IT-related findings are commonly raised in entities?

Answer:

1. The following outlines, and provides examples of, moderate and minor findings related to IT security management and user access:
   - Logging and monitoring of privileged user activity.
     - Inadequate design of controls, such as the scope of access being monitored and the independence of those monitoring activities.
     - Monitoring had not been performed in accordance with the entities' policies and procedures.
   - User access management, including approving new user access and performing regular user access reviews.
     - Managing access security configurations and user access reviews were not being performed in accordance with the entity's policies and procedures across several systems.
   - Removal of user access when it is no longer required.
     - Access being performed by users who no longer had a business requirement, including those who had ceased employment.
     - Insufficient controls for identifying and investigating access by users post cessation of their employment or contract.
     - Delays in the removal of user access.
   - Password configuration.
     - Passphrases used for single-factor authentication were not a minimum of 14 characters with complexity, and no risk assessment had been undertaken to determine the impact of not implementing the ISM recommended settings.

- Restricting access to financial and business data, and security configurations.
    - Inability to manage unauthorised access or modification of personally identifiable information. These included: limited ability to discover systems that contain information that would be classified as personally identifiable information; and no systematic method for tracking changes, access or distribution of personally identifiable information management of access to sensitive business data.
    - Security configurations that restrict access to sensitive functions are not implemented.
- Other commonly raised IT-related findings are:
    - Weaknesses in the operation of the change management processes.
        - restricting developer access to production systems and data.
        - segregation of duties between developers and migrators.
        - management of batch processing and reporting data.
    - Disaster recovery plans are not in place and/or not regularly tested.

Joint Committee of Public Accounts and Audit

Answers to Questions on Notice

Inquiry into Commonwealth Financial Statements 2021–22

Department/Agency: Australian National Audit Office
Topic: Protective Security Policy Framework (PSPF)
Date of Hearing: 19 May 2023
Type of question: Written
Date set by the committee for the return of answer: Friday 2 June 2023

Number of pages: 1

Question:
5. What are the implications for Cybersecurity if user access is not terminated in a timely manner?

6. Has the ANAO ever seen these risks materialise?

Answer:

1. A user account that has not had access appropriately removed could be compromised and used to by-pass other controls, gain unauthorised access to systems and data, and contribute to data exfiltration or data leakage.
2. The PSPF notes that 'International examples demonstrate that incidents of insiders compromising resources can occur after an individual has ceased employment. Therefore, separation measures are vital to limit these risks'.[1]
3. The ANAO has identified a number of instances where access was undertaken by users after separation from an entity where entities did not detect or adequately investigate the access performed[2][3].

[1] Protective Security Policy Framework, *Policy 14: Separating Personnel*, available from pspf-policy-14-separating-personnel.pdf (protectivesecurity.gov.au)

[2] Auditor-General Report No.8 2022-23 *Audits of the Financial Statements of Australian Government Entities for the Period Ended 30 June 2022* contains further details in the chapter 4 contributions for the following entities: Australian Nuclear Science and Technology Organisation, Attorney-General's Department, Departments of: Education, Skills and Employment; Infrastructure, Transport, Regional Development and Communications; Social Services; and Veterans' Affairs, and National Disability Insurance Agency.

[3] Auditor-General Report No.26 2022-23 Interim Report on Key Financial Controls of Major Entities contains further details in the chapter 3 contributions for the following entities: Attorney-General's Department, Departments of: Defence; Education; Employment and Workplace Relations; Finance; Infrastructure, Transport, Regional Development, Communications and the Arts; Social Services; Veterans' Affairs, and National Disability Insurance Agency.

OFFICIAL

Joint Committee of Public Accounts and Audit

Answers to Questions on Notice

Inquiry into Commonwealth Financial Statements 2021–22

Department/Agency: Australian National Audit Office
Topic: Protective Security Policy Framework (PSPF)
Date of Hearing: 19 May 2023
Type of question: Written
Date set by the committee for the return of answer: Friday 2 June 2023

Number of pages: 2

Question:

8. Issues with IT security management and user access have been repeatedly raised by the ANAO in previous financial statements audits, as well as performance audits. What more can be done to ensure that entities comply with the requirements of the framework?

9. What role does cybersecurity culture have in improving compliance with the framework requirements?

10. What can be done to lift the capability across the APS in relation to cybersecurity and IT skill more broadly?

Answer:

1. The ANAO does not provide detailed advice on management frameworks as this would impact independence when an audit is then undertaken on an activity subject to the framework.
2. The ANAO has previously noted that the current framework to support responsible Ministers in holding entities accountable within government is not sufficient to drive improvements in the implementation of mandatory requirements in relation to the implementation of the PSPF requirements[1]. This is also relevant in the implement of appropriate IT security controls to support the production of financial statements.
3. Cyber security culture can play a significant role in improving compliance with framework requirements. Establishing and embedding cyber security in behaviours and practices across governance and risk management, roles and responsibilities, technical support and monitoring of compliance ensures entities implement fit-for-purpose cyber security risk management frameworks to support their operations. This was demonstrated during the cyber audit of the Reserve Bank of Australia and ASC Pty Ltd.[2]

[1] Auditor-General Report No.32 2020-21 *Cyber Security Strategies of Non-Corporate Commonwealth Entities*
[2] Auditor-General Report No.1 2019-20 *Cyber Resilience of Government Enterprises and Corporate Entities*

4. Policy 2: *Management structures and responsibilities* of the PSPF includes a requirement to foster a positive security culture[3], in recognition that:

   Fostering a positive protective security culture is critical to achieving security outcomes. Through a robust security culture, the threat to an entity and its assets can be significantly decreased.

5. The following may assist in ensuring that framework requirements are met and in lifting capability across the APS.
   - Governance and risk management
     - Entities should establish assurance arrangements within management processes to assist with monitoring compliance against the PSPF and entity policies.
     - Entities should define appropriate guidance for assessing cyber security risks, including within procurements and contracts.
     - Entities should implement a framework to guide appropriate levels of engagement between business areas and cyber security specialists.
   - Learn from others
     - Entities should seek to learn from others (both from within and outside their organisation) who have similar environments or undertaken similar implementations, and from those who have expertise in cyber security to build on their knowledge and skill base.

[3] Protective Security Policy Framework Policy 2: Management structures and responsibilities, available from PSPF-policy-2-Management-structures-and-responsibilities.pdf (protectivesecurity.gov.au)

OFFICIAL

Joint Committee of Public Accounts and Audit

Answers to Questions on Notice

Inquiry into Commonwealth Financial Statements 2021–22

Department/Agency: Australian National Audit Office
Topic: Protective Security Policy Framework (PSPF)
Date of Hearing: 19 May 2023
Type of question: Written
Date set by the committee for the return of answer: Friday 2 June 2023

Number of pages: 1

Question:
How accurate are the self-assessments conducted by entities regarding their level of effectiveness in removing user access?

Answer:

1. As at 30 June 2021, 80% of 97 non-corporate commonwealth entities assessed themselves as being fully effective or higher at removing access 'On separation or transfer, the entity removed personnel's access to Australian Government resources, including physical facilities and ICT systems'. As at 30 June 2022 this self-reported figure increased to 82%.
2. As at 30 June 2022 there were three entities that were reported to have a moderate risk finding related to the removal of user access and reported being fully effective or higher.
3. As at the interim audit for 2022-23 eight of the 20 entities reviewed that reported being fully effective or higher as at 30 June 2022 had either a moderate or minor finding related to the removal of user access.[1]

[1] The control environment for these entities may have deteriorated since the last PSPF assessment.

OFFICIAL

Joint Committee of Public Accounts and Audit

Answers to Questions on Notice

Inquiry into Commonwealth Financial Statements 2021–22

Department/Agency: Australian National Audit Office
Topic: Protective Security Policy Framework (PSPF)
Date of Hearing: 19 May 2023
Type of question: Written
Date set by the committee for the return of answer: Friday 2 June 2023

Number of pages: 1

Question:
How does the ANAO collaborate with the Attorney-General's Department and the Australian Cyber Security Centre to improve the effectiveness of controls and mitigate risks related to user access and cybersecurity in government entities?

Answer:

1. The ANAO regularly meets with the Australian Cyber Security Centre (ACSC) to discuss the emerging IT security risks across the program of audits. The ACSC provides high-level advice on the cyber security landscape and various ACSC initiatives and activities.
2. The ANAO discusses the content of its cyber audit reports with the ACSC to assist in appropriately balancing the interests of accountability and potential risk exposure through transparent audit reporting.