

Management of Cyber Security Incidents

Australian Transaction Reports and Analysis Centre

Services Australia

© Commonwealth of Australia 2024

ISSN 1036–7632 (Print)

ISSN 2203–0352 (Online)

ISBN 978-1-76033-933-3 (Print)

ISBN 978-1-76033-934-0 (Online)

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

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

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

For terms of use of the Commonwealth Coat of Arms, visit the *Australian honours system* website at <https://www.pmc.gov.au/honours-and-symbols/australian-honours-system>.

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

Chief Operating Officer
Corporate Management Group
Australian National Audit Office
GPO Box 707
Canberra ACT 2601

Or via email:

communication@anao.gov.au.





Canberra ACT
14 June 2024

Dear President
Dear Mr Speaker

In accordance with the authority contained in the *Auditor-General Act 1997*, I have undertaken an independent performance audit in the Australian Transaction Reports and Analysis Centre and Services Australia. The report is titled *Management of Cyber Security Incidents*. Pursuant to Senate Standing Order 166 relating to the presentation of documents when the Senate is not sitting, I present the report of this audit to the Parliament.

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

Yours sincerely

A handwritten signature in black ink, reading 'Rona Mellor'.

Rona Mellor PSM
Acting 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 their 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
Email: ag1@anao.gov.au

Auditor-General reports and information about the ANAO are available on our website:
<http://www.anao.gov.au>

Audit team

Elijah Phal
Joanna Giang
Stevan Serafimov
Kelvin Le
Jason Ralston
Jade J. Koay
Sam Khaw
Edwin Apoderado
Xiaoyan Lu
Lesa Craswell

Contents

Summary and recommendations.....	7
Background	7
Conclusion	9
Supporting findings.....	10
Recommendations.....	12
Summary of entity responses.....	16
Key messages from this audit for all Australian Government entities.....	17
Audit findings.....	19
1. Background	20
Introduction.....	20
Management of cyber security incidents.....	22
Rationale for undertaking the audit	24
Audit approach	29
2. Australian Transaction Reports and Analysis Centre's cyber security incident management.....	30
Does AUSTRAC have appropriately designed and implemented cyber security incident management procedures?	32
Has AUSTRAC effectively implemented cyber security incident management processes for investigating, monitoring and responding to cyber security incidents?.....	41
Has AUSTRAC effectively implemented recovery processes that mitigate disruptions during and after cyber security incidents?.....	50
3. Services Australia's cyber security incident management	58
Does Services Australia have appropriately designed and documented cyber security incident management procedures?	60
Has Services Australia effectively implemented cyber security incident management processes for investigating and responding to cyber security incidents?.....	71
Has Services Australia effectively implemented recovery processes that mitigate disruptions during and after cyber security incidents?.....	79
Appendices	89
Appendix 1 Entity responses	90
Appendix 2 Improvements observed by the ANAO	94
Appendix 3 PSPF Policies 2, 4, 5 and 10 — requirements	95
Appendix 4 ASD's Cyber Security Guidelines — recommendations.....	98
Appendix 5 ASD's Essential Eight Maturity Model	100
Appendix 6 PSPF Self-Assessment Maturity Model.....	101



Audit snapshot

Auditor-General Report No.38 2023–24 Management of Cyber Security Incidents



Why did we do this audit?

- ▶ Australian Government entities are expected to be 'cyber exemplars' as they process and store some of Australia's most sensitive data to support the delivery of essential public services.
- ▶ Previous audits identified low levels of cyber resilience in non-corporate Commonwealth entities (NCEs).
- ▶ Low levels of cyber resilience make entities more susceptible to cyberattack and reduce business continuity and recovery prospects following a cyber security incident. Preparedness to respond to and recover from a cyberattack is a key part of cyber resilience.



What did we find?

- ▶ The implementation of arrangements by the Australian Transaction Reports and Analysis Centre (AUSTRAC) and Services Australia to manage cyber security incidents has been partly effective.
- ▶ AUSTRAC and Services Australia have partly designed and implemented cyber security incident management procedures.
- ▶ AUSTRAC and Services Australia have partly implemented effective cyber security incident management responses to investigate and respond to cyber security incidents.
- ▶ AUSTRAC and Services Australia have partly implemented effective cyber security incident management recovery to mitigate disruptions to business operations during and after cyber security incidents.



Key facts

- ▶ The Protective Security Policy Framework (PSPF) Policies 2, 4, 5 and 10 outline the requirements for the effective management of cyber security incidents.
- ▶ Supporting the PSPF are the relevant Australian Signals Directorate (ASD) Cyber Security Guidelines as well as ASD's *Essential Eight Maturity Model*.
- ▶ It is mandatory for NCEs to report the level of their security maturity each financial year.



What did we recommend?

- ▶ There were 19 recommendations aimed at improving the effective management of cyber security incidents.
- ▶ AUSTRAC agreed to nine recommendations. Services Australia agreed to 10 recommendations.

31%

of cyber security incidents reported to ASD were by Australian Government entities in 2022–23.

71%

of NCEs self-assessed at Maturity Level Two for the Essential Eight mitigation strategy, Regular backups.

82%

of NCEs self-assessed that they had an incident response plan in place, which was an increase from 2022.

Summary and recommendations

Background

1. New and emerging technologies play an important role in delivering digital services for Australian Government entities. As the development, integration and use of technology increases, so does the number of possible entry or weak points that malicious cyber actors can exploit. This is commonly referred to as the ‘attack surface’.¹ It is important that Australian Government entities continue to uplift their cyber security maturity and implement arrangements to manage cyber security incidents² effectively. The ability to maintain business continuity following a cyber security incident is critical to ensuring the continued provision of government services.

2. Australian Government entities are attractive, high-value targets for a range of malicious cybercriminals because they hold the personal and financial information of Australians.³ In 2022–23, approximately 31 per cent of cyber security incidents reported to the Australian Signals Directorate (ASD) were from non-corporate Commonwealth entities. Over 40 per cent of these cyber security incidents were coordinated, low-level malicious cyberattacks directed specifically at the Australian Government, government shared services, or regulated critical infrastructure.⁴ Ransomware was the most destructive cybercrime threat in 2022–23⁵ and continues to pose considerable risk to Australian Government entities, businesses and individuals.

Rationale for undertaking the audit

3. On 22 November 2023, the Australian Government released the *2023–30 Australian Cyber Security Strategy* which outlines a forecast approach towards uplifting Australia’s cyber resilience as well as ‘[building] ... national cyber readiness [and] proactively identifying and closing gaps in ... cyber defences and incident response plans’.

4. Australian Government entities are expected to be ‘cyber exemplars’, as they receive, process and store some of Australia’s most sensitive data to support the delivery of essential

1 An attack surface is ‘the amount of ICT equipment and software used in a system’. The greater the attack surface the greater the chances of a malicious actor finding an exploitable vulnerability. See Australian Signals Directorate, *ASD Cyber Threat Report 2022–23*, ASD, Canberra, 2023, available from <https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf> [accessed 8 April 2024], p. 11.

2 The Australian Signals Directorate defines a cyber security incident as an ‘an unwanted or unexpected cyber security event, or a series of such events, that has either compromised business operations or has a significant probability of compromising business operations’. See Australian Signals Directorate, ‘Guidelines for Cyber Security Incidents’ webpage, ASD, last updated March 2024, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents> [accessed on 8 April 2024].

3 Department of Home Affairs, *2023–2030 Australian Cyber Security Strategy*, Home Affairs, Canberra, 2023, <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf> [accessed 8 April 2024], p. 8.

4 See Australian Signals Directorate, *ASD Cyber Threat Report 2022–2023*, ASD, Canberra, 2023, <https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023> [accessed 22 November 2023], p. 8.

5 *ibid.*, p. 38.

public services.⁶ Whilst there were reported improvements from 2022, ASD's *2023 Cyber Security Posture Report* highlighted that the overall maturity level across entities remained low in 2023.⁷

5. Previous audits conducted by the ANAO identified low levels of cyber resilience in entities. Low levels of cyber resilience continue to make entities susceptible to cyberattack and reduce business continuity and recovery prospects following a cyber security incident. An entity's preparedness to respond to and recover from a cyberattack is a key part of cyber resilience. This audit was conducted to provide assurance to Parliament about the effectiveness of the selected entities' implementation of arrangements for managing cyber security incidents.

Audit objective, criteria and scope

6. The objective of this audit was to assess the effectiveness of the selected entities' implementation of arrangements for managing cyber security incidents in accordance with the Protective Security Policy Framework (PSPF) and relevant ASD Cyber Security Guidelines.

7. To form a conclusion against the audit objective, the following high-level criteria were adopted:

- Do the Australian Transaction Reports and Analysis Centre (AUSTRAC) and Services Australia have appropriately designed and implemented cyber security incident management procedures?
- Have AUSTRAC and Services Australia effectively implemented cyber security incident management processes for investigating, monitoring and responding to cyber security incidents?
- Have AUSTRAC and Services Australia effectively implemented recovery processes that mitigate disruptions during and after cyber security incidents?

Engagement with the Australian Signals Directorate

8. Independent timely reporting on the implementation of the cyber security policy framework supports public accountability by providing an evidence base for the Parliament to hold the executive government and individual entities to account. Previous ANAO reports on cyber security have drawn to the attention of Parliament and relevant entities the need for change in entity implementation of mandatory cyber security requirements, at both the individual entity and framework levels.

9. In preparing audit reports to the Parliament on cyber security in Australian Government entities, the interests of accountability and transparency must be balanced with the need to manage cyber security risks. ASD has advised the ANAO that adversaries use publicly available information about cyber vulnerabilities to more effectively target their malicious activities.

6 In December 2022, the Minister for Home Affairs appointed an Expert Advisory Board to assist and advise on the development of the Cyber Security Strategy. The three board members were Andrew Penn AO, Mel Hupfeld AO DSC, and Rachael Falk. The Expert Advisory Board published a discussion paper in February 2023. See Expert Advisory Board, *2023–2030 Australia Cyber Security Strategy – Discussion Paper*, Home Affairs, Canberra, 2023, available from https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf [accessed on 8 April 2024], p. 19.

7 Australian Signals Directorate, *The Commonwealth Cyber Security Posture Report in 2023*, ASD, Canberra, November 2023, available from <https://www.cyber.gov.au/sites/default/files/2023-11/Commonwealth-Cyber-Security-Posture-November-2023.pdf> [accessed 8 April 2024], p. 2.

10. The extent to which this report details the cyber security vulnerabilities of individual entities was a matter of careful consideration during the course of this audit. To assist in appropriately balancing the interests of accountability and potential risk exposure through transparent audit reporting, the ANAO engaged with ASD to better understand the evolving nature and extent of risk exposure that may arise through the disclosure of technical information in the audit report. This report therefore focusses on matters material to the audit findings against the objective and criteria and contains less detailed technical information than previous audits. Detailed technical information flowing from the audit was provided to the relevant accountable authorities during the audit process to assist them to gain their own assurance that their remediation plans are focussed on improving cyber resilience as required and support reliable reporting through the existing cyber security policy framework.

Conclusion

11. The implementation of arrangements by AUSTRAC and Services Australia to manage cyber security incidents has been partly effective. Neither entity is well placed to ensure business continuity or disaster recovery in the event of a significant or reportable cyber security incident.

AUSTRAC

12. AUSTRAC has partly effective cyber security incident management procedures for investigating, monitoring and responding to cyber security incidents. It has established management structures and a framework of procedures to support these processes. It has not detailed the responsibilities for its Chief Information Security Officer (CISO), its approach to continuous monitoring and improvement reporting, or defined timeframes for reporting to stakeholders.

13. AUSTRAC has partly implemented effective response processes that mitigate disruptions during and after cyber security incidents. It has established a Security Information and Event Management (SIEM) solution and processes for reporting cyber security incidents. The coverage of log events is not in accordance with ASD's Cyber Security Guidelines. AUSTRAC does not have an event logging policy and does not document its analysis of all cyber security events.

14. AUSTRAC has procedures to support its cyber security incident recovery processes. These procedures do not include the security and testing of backup solutions, nor detail the systems, applications and servers supporting critical business processes. AUSTRAC performs recovery of backups as part of business area requests. It does not perform testing of restoration of backups for disaster recovery purposes.

Services Australia

15. Services Australia is partly effective in its design of cyber security incident management procedures. It has established a framework of procedures and an incident response plan. It has not documented an approach to threat and vulnerability assessments. Services Australia does not have a policy covering the management of cyber security incidents.

16. Services Australia has partly effective cyber security incident response procedures for investigating and responding to cyber security incidents. It has procedures for managing data spills, malicious code infections and external instructions. It has implemented a Security

Information and Event Management (SIEM) solution and a systematic approach to monitoring and prioritisation of alerts. Services Australia has not established a timeframe for triage and escalation activities nor a process for analysing archived SIEM data. Services Australia has not defined an approach for cyber security investigations.

17. Services Australia has partly implemented effective recovery processes that mitigate disruptions during and after cyber security incidents. It has developed business continuity and disaster recovery plans and implemented regular backups. Its plans do not include all systems and applications supporting critical business processes and it does not test the recoverability of backups.

Supporting findings

AUSTRAC

18. AUSTRAC has established management structures and responsibilities for managing cyber security incidents. However, it has not documented the assigned responsibilities for its CISO although the CISO is empowered to make decisions. AUSTRAC has documented a framework of procedures for cyber security risk and incident management. However, it does not detail a process for reviewing, updating and testing its cyber security incident management procedures, nor has it implemented a security maturity monitoring plan that details an approach that defines a continuous improvement cycle as well as reporting to management. AUSTRAC has developed reporting processes for significant or reportable cyber security incidents. AUSTRAC does not document cyber security incident meetings, nor has it defined timeframes for reporting to relevant stakeholders. (See paragraphs 2.6 to 2.32)

19. AUSTRAC has reporting processes for reporting significant or reportable cyber security incidents to internal and external stakeholders. These processes do not include the engagement of relevant expertise in other business areas, such as legal advisors, and do not ensure the integrity of evidence supporting cyber security investigations. AUSTRAC has documented cyber security incident monitoring and response procedures. It has not developed an event log policy for handling and containing malicious code infections or intrusions, or containment actions in the event of a data spill. AUSTRAC has implemented a Security Information and Event Management (SIEM) solution. Its coverage of event logs is not in accordance with ASD's Cyber Security Guidelines. It undertakes an analysis of event logs and escalates significant or reportable cyber security incidents to management and relevant external stakeholders. It does not record or document its analysis of non-significant cyber security events, nor has it defined timeframes for triage and escalation activities. AUSTRAC is able to analyse data within its SIEM solution, it does not have a process for retrieving and analysing production and archived SIEM data. (See paragraphs 2.33 to 2.65)

20. AUSTRAC has documented procedures to support its cyber security incident recovery processes. These procedures do not include the security and testing of backup solutions, nor detail the systems, applications and servers supporting critical business processes. AUSTRAC has not tested the recoverability of its systems and applications supporting critical business processes. It has not included all relevant systems, including the tools used for managing backups, within disaster recovery testing schedules and security policies. AUSTRAC is not well placed to ensure business continuity or disaster recovery in the event of a significant or reportable cyber

security incident. AUSTRAC has primary and secondary data centres to support its approach to regular backups. AUSTRAC performs recovery of backups as part of business area requests. It does not perform testing of restoration of backups for disaster recovery purposes. It does not have a process for extracting and analysing production and archive backup data. AUSTRAC's incident reports include post-incident learning and post-remediation analysis. These reports are not used to review or update existing cyber security recovery procedures, with potential improvements highlighted in these reports not being considered for incorporation into existing cyber security documentation. (See paragraphs 2.66 to 2.93)

Services Australia

21. Services Australia has established management structures and responsibilities for its management of cyber security incidents. It has not documented an approach to threat and vulnerability assessments, nor does it have a policy covering the management of cyber security incidents but it does have a security maturity monitoring plan although this does not detail an approach that defines a continuous improvement cycle as well as reporting to management. Services Australia has developed a cyber security incident response plan and a trusted insider program. However, its trusted insider program has not considered input from other business areas, such as its legal function. Services Australia's critical asset and data registers do not have complete information on critical systems and data assets. Services Australia has documented a framework of procedures for cyber security risk and incident management. However, it does not detail a process for reviewing, updating and testing its cyber security incident management procedures. Services Australia has reporting processes that provide regular reporting of cyber security incidents, including significant or reportable cyber security incidents, to internal and external stakeholders. It has not defined the timeframes for reporting to relevant stakeholders and the consideration of engaging other relevant expertise, such as legal advisors, during reporting processes. (See paragraphs 3.6 to 3.44)

22. Services Australia has documented its approach for managing data spills, malicious code infections and intrusions. It has not established processes for reviewing, updating and testing these cyber security incident response procedures. Services Australia has implemented a Security Information and Event Management (SIEM) solution and developed a systematic approach to the monitoring and prioritisation of security alerts. Services Australia has an Event Logging and Monitoring Policy. It has not established processes for extracting, retrieving and analysing archived SIEM data, nor has it defined the timeframe requirements for triage and escalation activities. Services Australia has not defined an approach for cyber security investigations. (See paragraphs 3.45 to 3.73)

23. Services Australia has not defined an approach to digital preservation related to cyber security incidents and regular backups and nor does it have business continuity or disaster recovery plans that address all systems, including the systems which support the critical recovery processes. It is not well placed to ensure business continuity or disaster recovery in the event of a significant or reportable cyber security incident. Services Australia has processes for performing regular backups. These processes do not include all platforms and Services Australia does not test the restoration of data, applications and settings from backups as part of disaster recovery exercises. Services Australia has not appropriately documented an embedded post-incident learning approach following a cyber security incident. Services Australia has not established a

process that leverages post-incident learnings to review and improve the effective implementation of arrangements to manage cyber security incidents. (See paragraphs 3.74 to 3.103)

Recommendations

Recommendation no. 1 Paragraph 2.24

Australian Transaction Reports and Analysis Centre develops and implements:

- (a) policies that define the responsibilities of the Chief Information Security Officer in accordance with the Protective Security Policy Framework requirements; and
- (b) a security maturity monitoring plan that defines a continuous improvement cycle as well as reporting to management, including documenting the determination of reporting frequency and escalation.

Australian Transaction Reports and Analysis Centre response:
Agreed.

Recommendation no. 2 Paragraph 2.31

Australian Transaction Reports and Analysis Centre develops and implements:

- (a) processes for ensuring cyber security incident meetings are documented;
- (b) timeframes for reporting to relevant external stakeholders; and
- (c) processes that ensure regular risk reporting to its portfolio minister and the Department of Home Affairs.

Australian Transaction Reports and Analysis Centre response:
Agreed.

Recommendation no. 3 Paragraph 2.41

Australian Transaction Reports and Analysis Centre develops and implements:

- (a) procedures that define assigned security roles and responsibilities for coordinating responses, including engagement of relevant expertise; and
- (b) processes for managing and maintaining evidence during and after cyber security investigations.

Australian Transaction Reports and Analysis Centre response:
Agreed.

- Recommendation no. 4**
Paragraph 2.47
- Australian Transaction Reports and Analysis Centre develops and implements:
- (a) an approach for containment actions that restrict access to data, systems and networks in the event of a data spill; and
 - (b) an event log policy for handling and containing malicious code infections or intrusions.
- Australian Transaction Reports and Analysis Centre response:**
Agreed.
- Recommendation no. 5**
Paragraph 2.57
- Australian Transaction Reports and Analysis Centre implements a strategy for Security Information and Event Management (SIEM) solution coverage that is in accordance with Australian Signals Directorate's *Guidelines for System Monitoring* and performs a risk assessment to support any deviations from the guideline's recommendations.
- Australian Transaction Reports and Analysis Centre response:**
Agreed.
- Recommendation no. 6**
Paragraph 2.63
- Australian Transaction Reports and Analysis Centre establishes:
- (a) a process for retrieving and analysing production Security Information and Event Management (SIEM) solution data held within its SIEM solution and archived SIEM data;
 - (b) record keeping requirements for triage and escalation activities over non-significant cyber security events to ensure completeness of activities; and
 - (c) timeframe requirements for triage and escalation activities.
- Australian Transaction Reports and Analysis Centre response:**
Agreed.
- Recommendation no. 7**
Paragraph 2.78
- Australian Transaction Reports and Analysis Centre develops and implements:
- (a) disaster recovery testing schedules that include backup solutions;
 - (b) business continuity planning processes that incorporate the systems, applications and servers which support critical business processes; and
 - (c) processes that test the recoverability of its systems and applications supporting critical business processes, including implementing any lessons learned into future testing schedules.
- Australian Transaction Reports and Analysis Centre response:**
Agreed.

- Recommendation no. 8
Paragraph 2.88** Australian Transaction Reports and Analysis Centre establishes a program that assesses the effectiveness of recovery processes for all production and archived backup data.
- Australian Transaction Reports and Analysis Centre response:**
Agreed.
- Recommendation no. 9
Paragraph 2.92** Australian Transaction Reports and Analysis Centre leverage its post-incident learning approaches following a cyber security incident to inform a process that reviews, updates and tests all of the relevant security documentation for the effective management of cyber security incidents. That is:
- (a) supporting security documentation to its security plans;
 - (b) framework of procedures for cyber security incident management;
 - (c) associated guidance for cyber security incident response; and
 - (d) associated guidance for cyber security incident recovery.
- Australian Transaction Reports and Analysis Centre response:**
Agreed.
- Recommendation no. 10
Paragraph 3.18** Services Australia updates its trusted insider program with the support of legal advice and other relevant expertise and ensure it is fit for purpose across the organisation.
- Services Australia response:** *Agreed.*
- Recommendation no. 11
Paragraph 3.23** Services Australia updates its systems criticality assessments and data registers with the necessary information to confirm the criticality of each system and data asset.
- Services Australia response:** *Agreed.*
- Recommendation no. 12
Paragraph 3.29** Services Australia establishes a Cyber Security Incident Management Policy or include 'cyber security incidents' as part of the scope of the Incident Management and Escalation Policy.
- Services Australia response:** *Agreed.*
- Recommendation no. 13
Paragraph 3.35** Services Australia develops and implements an approach that ensures continuous monitoring and improvement reporting is provided to management, including documenting the determination of reporting frequency and escalation.
- Services Australia response:** *Agreed.*

- Recommendation no. 14**
Paragraph 3.43
- Services Australia designs and implements procedures detailing:
- (a) the timeframes for reporting to internal and external stakeholders; and
 - (b) roles and responsibilities for coordinating responses, including engagement of relevant expertise.

Services Australia response: *Agreed.*

- Recommendation no. 15**
Paragraph 3.59
- Services Australia develops and implements procedures detailing:
- (a) the process for performing cyber security investigations in accordance with the Australian Government Investigations Standard; and
 - (b) the process for managing and maintaining evidence during and after cyber security investigations.

Services Australia response: *Agreed.*

- Recommendation no. 16**
Paragraph 3.71
- Services Australia develops and implements:
- (a) a process for retrieving and analysing archived Security Information and Event Management (SIEM) solution data; and
 - (b) timeframe requirements for triage and escalation activities.

Services Australia response: *Agreed.*

- Recommendation no. 17**
Paragraph 3.87
- Services Australia develop and implement:
- (a) a policy for digital preservation;
 - (b) a policy for regular backups;
 - (c) business continuity and disaster recovery plans that include the systems, applications and servers which support their critical recovery processes; and
 - (d) processes that test the recoverability of their systems and applications supporting critical business processes, and implement any lessons learned into future testing plans.

Services Australia response: *Agreed.*

- Recommendation no. 18**
Paragraph 3.96
- Services Australia establish a program that assesses the effectiveness of recovery processes for all production and archived backup data.

Services Australia response: *Agreed.*

Recommendation no. 19 Services Australia develops its post-incident learning approaches following a cyber security incident to inform a process that reviews, updates and tests all of the relevant security documentation for the effective management of cyber security incidents. That is:

Paragraph 3.101

- (a) supporting security documentation to their security plans;
- (b) framework of procedures for cyber security incident management;
- (c) associated guidance for cyber security incident response; and
- (d) associated guidance for cyber security incident recovery.

Services Australia response: *Agreed.*

Summary of entity responses

24. The proposed audit report was provided to AUSTRAC and Services Australia. The entities' summary responses are reproduced below. Their full responses are included at Appendix 1. Improvements observed by the ANAO during the course of this audit are listed at Appendix 2.

AUSTRAC

AUSTRAC welcomes the review and the opportunity to reflect on its processes and procedures for managing cybersecurity incidents. AUSTRAC maintains that our processes to date have enabled effective management of cyber security incidents if and as they occur, involving prioritisation, escalation and seeking internal and external expertise to inform AUSTRAC's effective cyber security incident response. AUSTRAC welcomes the ANAO's recommendations, which will support AUSTRAC to strengthen our approach to cybersecurity incident management through greater clarity and certainty provided by documenting much of our existing approach and enhancing it where gaps have been identified. In response to the recommendations, AUSTRAC will update key incident response plans and documents, as well as develop testing schedules consistent with our risk profile and appetite and operational requirements.

Services Australia

Services Australia (the Agency) notes the audit findings and the recommendations for the Agency associated with improving the management of cyber security. The Agency agrees with the recommendations, and will work towards further strengthening controls in the identified areas.

The Agency takes its responsibility to safeguard the personal information and data of its customers very seriously, as well as the need to ensure continuity of the essential services and payments that the Agency provides. I consider that the implementation of the recommendations contained in the report will support the Agency in achieving those outcomes.

Key messages from this audit for all Australian Government entities

25. Below is a summary of key messages, including instances of good practice, which have been identified in this audit and may be relevant for the operations of other Australian Government entities.

Governance and risk management

- Public services are increasingly reliant on the availability of systems. Entities should understand and assess the need for critical business continuity and disaster recovery management and frame their security documentation and processes on the basis that cyber security incidents could disrupt or shut down the delivery of digital services to the Australian public.
- Entities should document policies and procedures — which is important for managing staff turnover — particularly for smaller organisations that are critically dependent on the qualifications and experience of key security advisors.
- Entities should leverage post-incident learning to inform a process that reviews, updates and tests all security documentation for the effective management of cyber security incidents. Post-incident learning greatly improves business continuity and recovery prospects following a significant or reportable cyber security incident.
- Entities should implement a trusted insider program which would actively assist an entity to effectively detect and mitigate internal cyberattack threats.
- As Australia’s cyber security regulatory landscape evolves and reforms, it is important for an entity to consider how their legal function will support their governance committees during the external reporting process to manage increasing scrutiny and liability risks following a significant or reportable cyber security incident.

Performance and impact measurement

- Entities should implement a systematic and centralised approach to the management of Security Information and Event Management (SIEM) solutions, including automated monitoring and prioritisation of security alerts.

Audit findings

1. Background

Introduction

1.1 New and emerging technologies play an important role in delivering digital services for Australian Government entities. As the development, integration and use of technology increases, so too does the number of possible entry or weak points that malicious cyber actors can exploit. This is commonly referred to as the ‘attack surface’.⁸ It is important that Australian Government entities continue to uplift their cyber security maturity and implement arrangements to manage cyber security incidents effectively.⁹ The ability to maintain business continuity following a cyber security incident is critical to ensuring the continued provision of government services.

1.2 Cyberattacks on Optus and Medibank in 2022 caused large-scale data breaches which ‘exposed the gaps in Australia’s existing incident response functions’ and highlighted the critical importance of effective cyber security incident management.¹⁰ Following this, the role of the National Cyber Security Coordinator was established to:

lead national cyber security policy, the coordination of responses to major cyber [security] incidents, [whole-of-government] cyber incident preparedness efforts and strengthening of Commonwealth cyber security capability.¹¹

1.3 In September 2023, an investigation by the National Cyber Security Coordinator into another large-scale data breach involving HWL Ebsworth Lawyers¹² found that up to 65 Australian Government entities including Services Australia had been indirectly impacted. The National Cyber Security Coordinator concluded that¹³:

The attack on HWL Ebsworth provides important lessons for Government ... and insight into how we can more effectively respond to and rebound from future cyber [security] incidents.

8 An attack surface is ‘the amount of ICT equipment and software used in a system’. The greater the attack surface the greater the chances of a malicious actor finding an exploitable vulnerability. See Australian Signals Directorate, ASD Cyber Threat Report 2022–23, ASD, Canberra, 2023, available from <https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023> [accessed 8 April 2024].

9 The Australian Signals Directorate defines a cyber security incident as an ‘an unwanted or unexpected cyber security event, or a series of such events, that has either compromised business operations or has a significant probability of compromising business operations’. See Australian Signals Directorate, ‘Guidelines for Cyber Security Incidents – Managing cyber security incidents’ webpage, last updated March 2024, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents> [accessed 8 April 2024].

10 In December 2022, the Minister for Home Affairs appointed an Expert Advisory Board to assist and advise on the development of the Cyber Security Strategy. The three board members were Andrew Penn AO, Mel Hupfeld AO DSC, and Rachael Falk. The Expert Advisory Board published a discussion paper in February 2023. Expert Advisory Board, *2023–2030 Australian Cyber Security Strategy – Discussion Paper*, Department of Home Affairs, Canberra, 2023, available from <https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030-australian-cyber-security-strategy-discussion-paper.pdf> [accessed 8 April 2024], p. 20.

11 Prime Minister, Minister for Home Affairs, and Minister for Cyber Security, ‘Appointment of National Cyber Security Coordinator’, media release, Parliament House, Canberra, 23 June 2023.

12 HWL Ebsworth Lawyers is a full-service commercial law firm that operates throughout Australia.

13 Department of Home Affairs, ‘National Cyber Security Coordinator Statement on HWL Ebsworth’, media release, Home Affairs, 18 September 2023, available from <https://www.homeaffairs.gov.au/news-media/archive/article?itemid=1122> [accessed 8 April 2024].

1.4 Australian Government entities are attractive high-value targets for a range of malicious cybercriminals because they hold the personal and financial information of Australians.¹⁴ In 2022–23, approximately 31 per cent of cyber security incidents reported to the Australian Signals Directorate (ASD) were from Australian Government entities. Over 40 per cent of these cyber security incidents were coordinated low-level malicious cyberattacks directed specifically at federal government, government shared services or regulated critical infrastructure.¹⁵ Ransomware remains the most significant cybercrime threat in 2022–23¹⁶ and continues to pose considerable risk to Australian Government entities, businesses and individuals.

1.5 The Office of the Australian Information Commissioner’s *Notifiable Data Breaches Report: January to June 2023* outlined that¹⁷:

- sixty-seven per cent of notifiable data breach reports were cyber security incidents caused by malicious or criminal attacks;
- cyber security incidents continued to be the cause for a sizable proportion of large-scale data breaches; and
- more than 10 million Australians were affected for the first time since notifiable data breach reporting to the Office of the Australian Information Commissioner (OAIC) commenced on 22 February 2018.¹⁸

1.6 This biannual report identified that the top two sectors reporting notifiable data breaches were health service providers and finance including superannuation. The Australian Government entered the top five sectors reporting notifiable data breaches for the first time since the reporting period January to June 2021.

1.7 In ASD’s *2023 Cyber Security Posture Report*, 25 per cent of non-corporate Commonwealth entities (NCEs) self-assessed at Maturity Level Two across the Essential Eight mitigation strategies when implemented compensating controls were considered.¹⁹ Specifically, 71 per cent of these

14 Expert Advisory Board, *2023–2030 Australian Cyber Security Strategy – Discussion Paper*, available from https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030_australian_cyber_security_strategy_discussion_paper.pdf [accessed on 8 April 2024], p. 8.

15 Australian Signals Directorate, *ASD Cyber Threat Report 2022–2023*, ASD, Canberra, 2023, available from <https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf> [accessed 22 November 2023], p. 8.

16 *ibid.*, p. 38.

17 Office of the Australian Information Commissioner, *Notifiable Data Breaches Report: January to June 2023*, OAIC, available from https://www.oaic.gov.au/_data/assets/pdf_file/0021/156531/Notifiable-data-breaches-report-July-to-December-2023.pdf [accessed 8 April 2024], pp. 3, 5, and 11.

18 Attorney-General’s Department, ‘Rights and Protections – Privacy’ webpage, AGD, 2024, available from <https://www.ag.gov.au/rights-and-protections/privacy> [accessed 8 April 2024].

19 The Essential Eight are mitigation strategies recommended from ASD’s Strategies to Mitigate Cyber Security Incidents. See Australian Signals Directorate, ‘Essential Eight’ webpage, ASD, Canberra, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight> [accessed 9 April 2024].

A compensating control is a management, operational or technical control employed in lieu of a recommended control which provides equivalent or comparable protection.

NCEs self-assessed at Maturity Level Two for the Essential Eight mitigation strategy ‘Regular backups’.²⁰

1.8 In addition, 82 per cent of NCEs self-assessed that they had an incident response plan, which was reported as an improvement from 2022. Of these, 90 per cent indicated that their incident response plan had been last updated within the last two years and 69 per cent indicated that their incident response plan had been enacted at least every two years. There was a decrease in cyber security incident reporting to ASD compared to 2022 which ASD indicated may be due to NCEs experiencing a high number of low-impact cyber security incidents. The Protective Security Policy Framework (PSPF) only requires that NCEs report ‘significant or reportable’ cyber security incidents to ASD.²¹

Management of cyber security incidents

1.9 The requirements for NCEs to effectively implement arrangements for the management of cyber security incidents are specified in the PSPF and supported by the relevant ASD Cyber Security Guidelines.

Protective Security Policy Framework

1.10 Under the Directive on the Security of Government Business issued in October 2018, the PSPF was documented as an Australian Government policy for Australian Government entities.²² Specifically, NCEs who are subject to the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) must apply the PSPF to the extent consistent with legislation.²³ For corporate Commonwealth entities and wholly-owned Commonwealth companies subject to the PGPA Act, the PSPF represents better practice. This audit report will refer to the NCE entities that must apply the PSPF as ‘entities’, as is also used in the PSPF and supporting PSPF guidance.

1.11 The PSPF specifies the requirements for how entities can effectively implement arrangements for the management of cyber security incidents by reporting and recording; assessing and deciding; responding and recovering; and learning following a cyber security incident. These requirements are outlined across PSPF Policies 2, 4, 5 and 10 (see Appendix 3).²⁴

20 Entities self-assess against the Essential Eight Maturity Model, which sets out descriptions of the Essential Eight mitigation strategies at each maturity level. See paragraph 1.14, and Australian Signals Directorate, ‘Essential Eight Maturity Model’ webpage, ASD, Canberra, 2017 (last updated November 2023), available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model> [accessed on 8 April 2024].

21 Australian Signals Directorate, *The Commonwealth Cyber Security Posture Report in 2023*, ASD, Canberra, 2023, available from <https://www.cyber.gov.au/sites/default/files/2023-11/Commonwealth-Cyber-Security-Posture-November-2023.pdf> [accessed 27 November 2023], p. 15.

22 On 3 August 2023, the management of the PSPF transferred from the Attorney-General’s Department to the Department of Home Affairs as part of a machinery of government change. In October 2023, the Directive on the Security of Government Business was recertified and the PSPF was reaffirmed as Australian Government policy by the Minister for Home Affairs and the Minister for Cyber Security.

23 Department of Home Affairs, ‘Applying the Protective Security Policy Framework’ webpage, Home Affairs, available from <https://www.protectivesecurity.gov.au/about/applying-protective-security-policy-framework> [accessed 24 November 2023].

24 Department of Home Affairs, ‘Protective Security Policy Framework – Policies’ webpage, Home Affairs, available from <https://www.protectivesecurity.gov.au/policies> [accessed 8 April 2024].

1.12 It is mandatory for entities to report the level of their security maturity to the relevant portfolio minister and to the Department of Home Affairs each financial year using the PSPF's online reporting portal.²⁵ Entities must report across four protective security outcomes using the PSPF Maturity Self-Assessment Maturity Model (see Table 1.1 and Appendix 6). The Department of Home Affairs uses the reported data provided by entities to produce a consolidated view of the protective security maturity of entities. This is published within the annual PSPF Assessment Report by the Department of Home Affairs.

Table 1.1: PSPF Self-Assessment Maturity Model

PSPF Maturity Level	Maturity Level Description
Maturity Level One	Partial: Some PSPF core and supporting requirements are implemented although may not be well understood across the entity. The entity is not meeting security outcomes in some areas.
Maturity Level Two	Substantial: The majority of PSPF core and supporting requirements are implemented, broadly managed and understood across the entity. The entity is meeting security outcomes in most areas.
Maturity Level Three	Full: All PSPF core and supporting requirements are implemented, integrated into business practices and clearly understood across the entity. The entity is meeting security outcomes.
Maturity Level Four	Superior: All PSPF core and supporting requirements are implemented, comprehensively understood and embedded across the entity. Entity is implementing better practice, beyond PSPF requirements. The entity is exceeding security outcomes.

Source: ANAO summary of diagram in Department of Home Affairs' *PSPF Assessment Report 2022–23*, p. 4.

ASD's Cyber Security Guidelines and Essential Eight Maturity Model

1.13 Supporting the PSPF are the relevant ASD Cyber Security Guidelines. The guidelines are published in the *Information Security Manual*, which provides practical guidance on how entities can protect their systems and data from cyber threats.²⁶ The relevant ASD Cyber Security Guidelines are as follows:

- *Guidelines for Cyber Security Incidents* provides practical guidance on managing and responding to cyber security incidents²⁷;
- *Guidelines for Cyber Security Roles* outlines the role and responsibilities of the Chief Information Security Officer (CISO) when overseeing cyber security response activities and during business continuity and disaster recovery planning²⁸; and

25 Department of Home Affairs, 'Protective Security Policy Framework – Reporting' webpage, Home Affairs, available from <https://www.protectivesecurity.gov.au/reporting> [accessed 8 April 2024].

26 Australian Signals Directorate, 'Information Security Manual (ISM)' webpage, ASD, Canberra, last updated March 2024, Available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism> [accessed 8 April 2024].

27 Australian Signals Directorate, 'Guidelines for Cyber Security Incidents' webpage, ASD, Canberra, last updated on 1 March 2024, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents> [accessed 8 April 2024].

28 Australian Signals Directorate, 'Guidelines for Cyber Security Roles' webpage, ASD, Canberra, last updated 1 December 2023, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-roles> [accessed 8 April 2024].

- *Guidelines for System Monitoring* specifies how entities implement event logging and monitoring.²⁹

1.14 ASD's Essential Eight Maturity Model³⁰ provides advice on how to implement the Essential Eight mitigation strategies. Recommendations from ASD's Cyber Security Guidelines and the Essential Eight Maturity Model are set out at Appendices 4 and 5.

Rationale for undertaking the audit

1.15 On 22 November 2023, the Australian Government released the *2023–30 Australian Cyber Security Strategy* which outlines an approach towards uplifting Australia's cyber resilience as well as '[building] ... national cyber readiness by proactively identifying and closing gaps in our cyber defences and incident response plans'.³¹

1.16 Australian Government entities are expected to be 'cyber exemplars' given that they receive, process and store some of Australia's most sensitive data to support the delivery of essential public services.³² Whilst there were improvements from 2022, ASD's *2023 Cyber Security Posture Report* highlighted that the overall maturity level across entities remained low in 2023.³³ Previous audits conducted by the ANAO identified low levels of cyber resilience in entities.³⁴

1.17 Low levels of cyber resilience continue to make entities susceptible to cyberattack and reduces their business continuity and recovery prospects following a cyber security incident.³⁵ An entity's preparedness to respond to and recover from cyberattack is a key part of cyber resilience. This audit was conducted to provide assurance to Parliament about the effectiveness of the selected entities' implementation of arrangements for managing cyber security incidents.

1.18 The selected entities for this audit were the Australian Transaction Reports and Analysis Centre (AUSTRAC) and Services Australia. Both are NCEs that must apply the PSPF (see paragraph 1.10).

29 Australian Signals Directorate, 'Guidelines for System Monitoring' webpage, ASD, Canberra, last updated 1 December 2023, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-monitoring> [accessed 8 April 2024].

30 Australian Signals Directorate, 'Essential Eight Maturity Model' webpage, ASD, Canberra, last updated 27 November 2023, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model> [accessed 8 April 2024].

31 Department of Home Affairs, *2023–2030 Australian Cyber Security Strategy*, Home Affairs, Canberra, 2023, available from <https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf> [accessed 8 April 2024], p. 44.

32 Expert Advisory Board, *2023–2030 Australian Cyber Security Strategy – Discussion Paper*, available from <https://www.homeaffairs.gov.au/reports-and-pubs/files/2023-2030-australian-cyber-security-strategy-discussion-paper.pdf> [accessed 8 April 2024], p. 19.

33 Australian Signals Directorate, *The Commonwealth Cyber Security Posture Report in 2023*, ASD, Canberra, 2023, available from <https://www.cyber.gov.au/sites/default/files/2023-11/Commonwealth-Cyber-Security-Posture-November-2023.pdf> [accessed 8 April 2024], p. 2.

34 Auditor-General Report No.9 2022–23, *Management of Cyber Security Supply Chain Risks*, ANAO, Canberra, 2022, para 1.18, available from https://www.anao.gov.au/sites/default/files/2022-12/Auditor-General_Report_2022-23_9.pdf [accessed 29 January 2024].

35 Australian Signals Directorate, *2022–02: Australian organisations should urgently adopt an enhanced cyber security posture*, Advisory, ASD, Canberra, issued 23 February 2022, available from <https://www.cyber.gov.au/about-us/advisories/2022-02-australian-organisations-should-urgently-adopt-enhanced-cyber-security-posture> [accessed 29 January 2024].

1.19 The selection process for these entities included consideration of:

- the type of information held by the entity;
- the type of services provided by the entity; and
- whether the entity manages critical infrastructure or systems of national interest, such as those relating to financial services, health and welfare.

1.20 Table 1.2 sets out the key information holdings and service characteristics of AUSTRAC and Services Australia.

Table 1.2: Selected entities' information holdings and service characteristics

Entity	Economic or commercial information	Citizens' personal information	National security or critical infrastructure	Program and service delivery	Policy or regulatory
AUSTRAC	✓	✓	✓	✗	✓
Services Australia	✓	✓	✓	✓	✓

Note: Service characteristics were obtained from ASD.

Source: ANAO analysis of the entities' information holdings and service characteristics.

AUSTRAC

1.21 AUSTRAC operates in an environment shaped by new and emerging technologies as well as criminals who become more sophisticated and develop new ways to exploit vulnerabilities in Australia's financial system.³⁶

1.22 As Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regulator and Financial Intelligence Unit (FIU), AUSTRAC is responsible for detecting, deterring and disrupting criminal exploitation of the Australian financial system in order to protect the Australian community from serious and organised crime.³⁷

1.23 AUSTRAC's purpose is underpinned by the objectives of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act). This includes³⁸:

- supporting cooperation and collaboration with Commonwealth, state and territory law enforcement, revenue, border and national security intelligence entities to detect, deter and disrupt money laundering and terrorism financing (ML/TF) as well as other serious financial crimes;
- providing financial intelligence services information for the purposes of investigating and prosecuting ML/TF offences and other serious crimes;
- promoting public confidence in Australia's financial system; and

36 AUSTRAC, 'About Us' webpage, AUSTRAC, Canberra, available from <https://www.austrac.gov.au/about-us/what-we-do> [accessed 20 March 2024].

37 AUSTRAC, *AUSTRAC Annual Report 2022–23*, AUSTRAC, Canberra, 2023, available from <https://www.austrac.gov.au/sites/default/files/2023-10/AUSTRAC%20Annual%20Report%202023.pdf> [accessed on 8 April 2024], p. 14.

38 *ibid.*, p. 14.

- fulfilling Australia’s international obligations and address matters of international concern in combatting ML/TF.

1.24 AUSTRAC regulates more than 17,000 individuals, businesses and organisations to ensure they have robust AML/CTF processes and systems in place and to identify and mitigate ML/TF risks. In doing so, AUSTRAC receives almost half a million reports each day from businesses such as banks and credit unions, lenders and stockbrokers, gambling and bullion service providers, remittance dealers and digital currency exchange providers.³⁹

Services Australia

1.25 Services Australia operates in an environment shaped by new and emerging technologies as well as the ‘events of recent years, including the COVID-19 pandemic and a number of natural disasters and emergencies’ which has ‘transformed’ its business.⁴⁰

1.26 The role and function of Services Australia is to design, deliver, coordinate, and monitor government services and payments relating to social security, child support, students, families, aged care, health programs, and emergency and disaster payments.⁴¹ Practically, this includes:

- payments and services to assist with the cost of raising a child, including information about childcare and child support;
- assistance with living arrangements, such as information on moving house, relationship changes, and relocating to Australia;
- help and support for individuals affected by natural disasters or family and domestic violence;
- payments and services for retirees or those accessing aged care, along with support for individuals caring for older Australians; and
- assistance for individuals who have recently become unemployed, are seeking employment, or experiencing income changes.

1.27 Services Australia holds various types of social, health and welfare information to assist in the delivery of payments and services. This includes personal information related to confirming identity, communicating with individuals, providing advice and support, ensuring correct payments, managing complaints, investigating fraud, and exchanging data with other entities.⁴²

Selection of the entities

1.28 AUSTRAC and Services Australia were selected so that an assessment could be made of the cyber security incident management approach of:

39 *ibid.*, p. 15.

40 Services Australia, *Corporate Plan 2023–24*, Services Australia, Canberra, 2023, available from <https://www.servicesaustralia.gov.au/sites/default/files/2023-08/corporate-plan-23-24.pdf> [accessed 20 March 2024], p. 6.

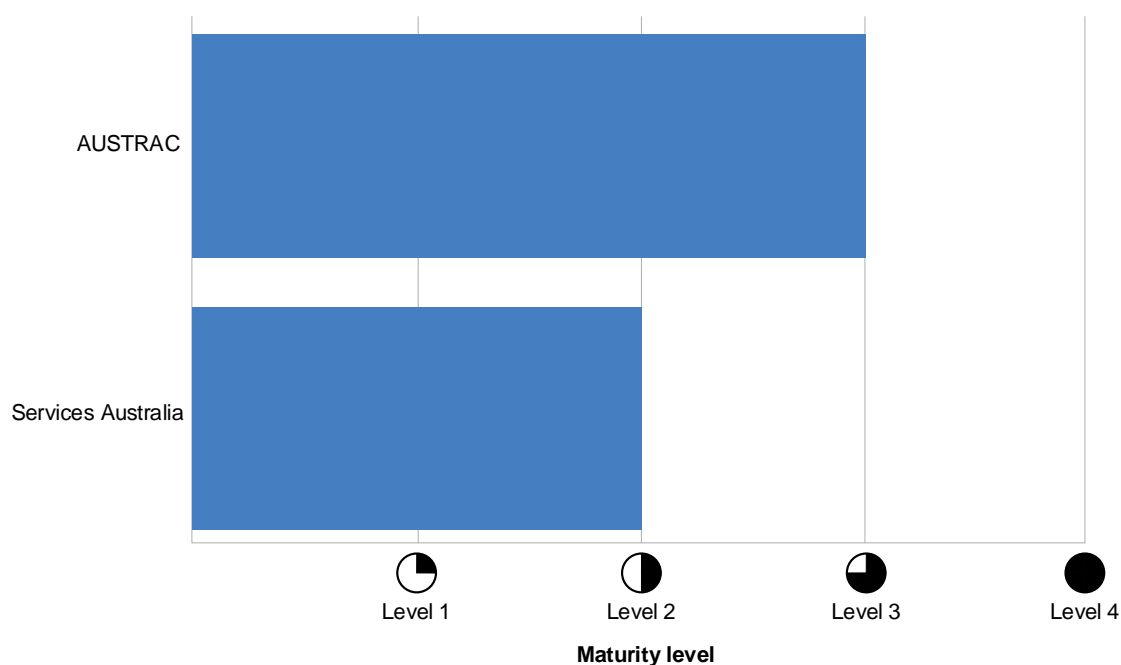
41 *ibid.*, p. 2.

42 Services Australia, ‘Privacy Policy’ webpage, Services Australia, Canberra, 2024, available from <https://www.servicesaustralia.gov.au/privacy-policy?context=1> [accessed 20 March 2024].

- a medium entity and an extra-large entity⁴³;
- an entity that holds financial intelligence information and an entity that holds the health and welfare information of Australians⁴⁴; and
- entities with varying PSPF maturity self-assessment levels across the relevant PSPF policies.

1.29 AUSTRAC's and Services Australia's overall PSPF maturity level across 2022–23 is outlined below (see Figure 1.1) and across the relevant PSPF Policies 2, 4, 5 and 10 (see Figure 1.2) as well as across financial years from 2019 to 2023 (see Figure 1.3).

Figure 1.1: Selected entities' reported overall PSPF maturity level, 2022–23

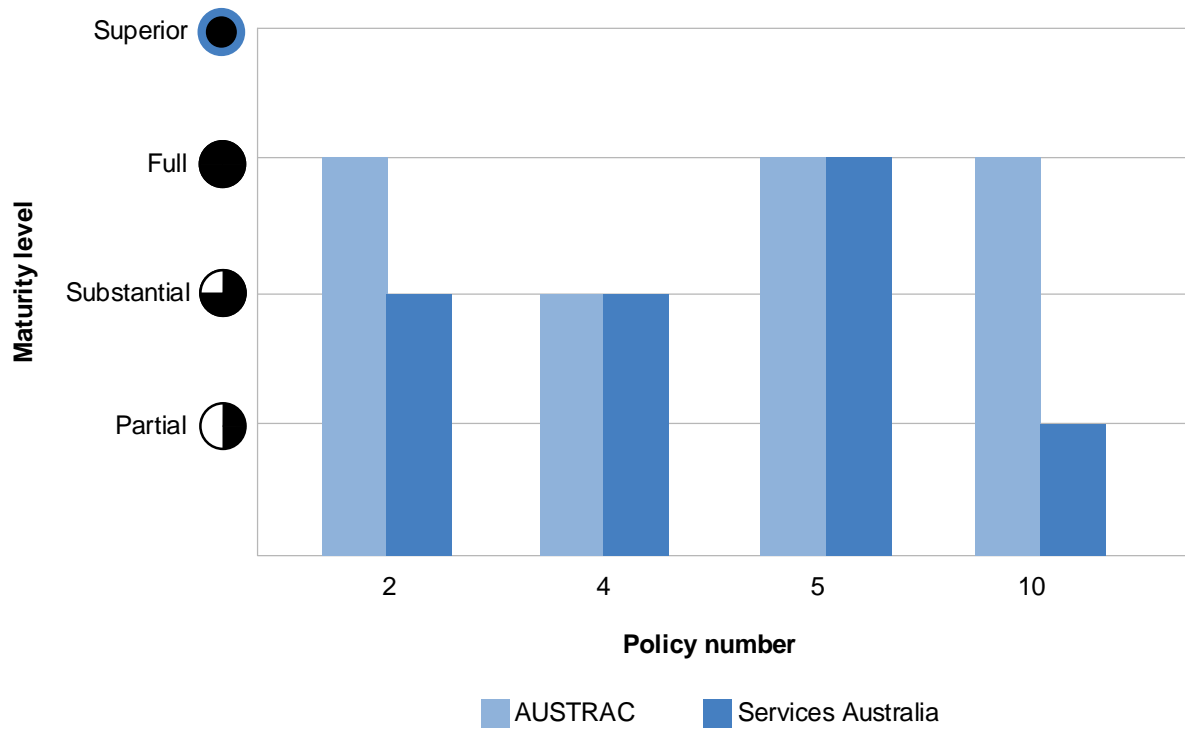


Source: ANAO analysis of PSPF Reporting Data for 2022–23.

43 Australian Public Service Commission, 'APS Agencies – size and function' webpage, APSC, Canberra, last updated February 2023, available from <https://www.apsc.gov.au/aps-agencies-size-and-function> [accessed 26 March 2024].

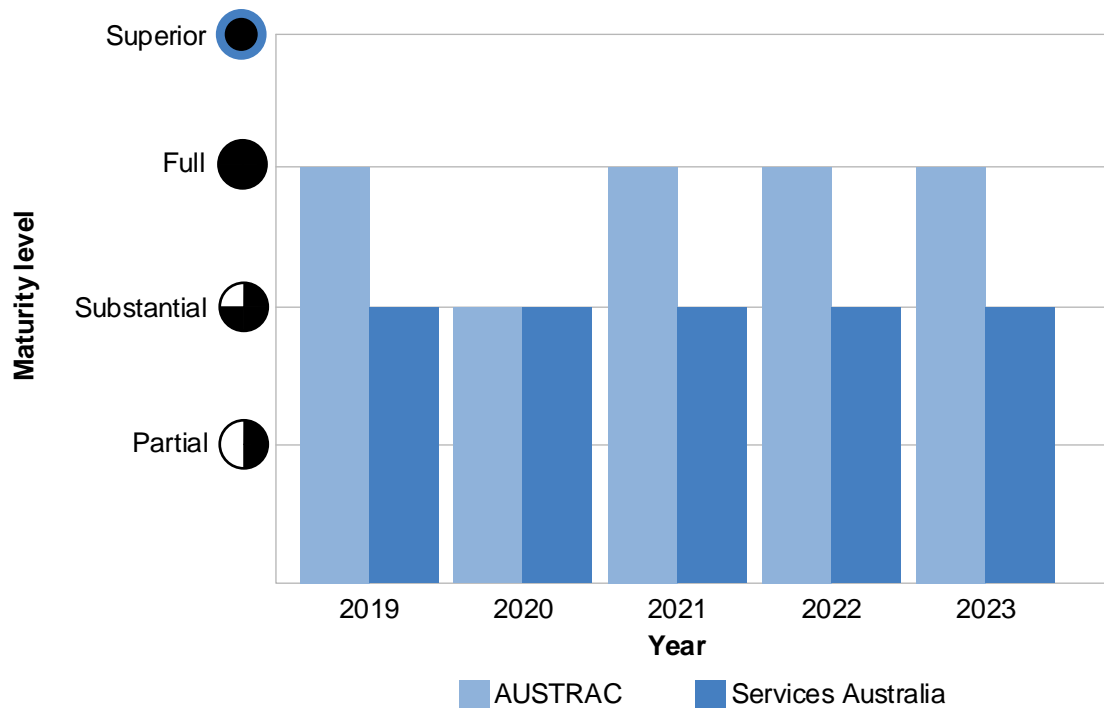
44 The OAIC *Notifiable Data Breaches Report July to December 2023* outlined that the top two sectors reporting notifiable data breaches to the OAIC were and health service providers and finance including superannuation. See Office of the Australian Information Commissioner, *Notifiable Data Breaches Report July to December 2023*, OAIC, Canberra, 2023, available from https://www.oaic.gov.au/data/assets/pdf_file/0021/156531/Notifiable-data-breaches-report-July-to-December-2023.pdf [accessed 8 April 2024].

Figure 1.2: Selected entities' reported overall PSPF maturity level for relevant policies, 2022–23



Source: ANAO analysis of PSPF Reporting Data for 2022–23.

Figure 1.3: Selected entities' reported overall PSPF maturity level from 2019 to 2023



Source: ANAO analysis of PSPF Reporting Data for 2019 to 2023.

Audit approach

Audit objective, criteria and scope

1.30 The objective of this audit was to assess the effectiveness of the selected entities' implementation of arrangements for managing cyber security incidents in accordance with the PSPF and relevant ASD Cyber Security Guidelines.

1.31 To form a conclusion against the audit objective, the ANAO adopted the following high-level criteria.

- Do AUSTRAC and Services Australia have appropriately designed and implemented cyber security incident management procedures?
- Have AUSTRAC and Services Australia effectively implemented cyber security incident management processes for investigating, monitoring and responding to cyber security incidents?
- Have AUSTRAC and Services Australia effectively implemented recovery processes that mitigate disruptions during and after cyber security incidents?

Audit methodology

1.32 The audit methodology included:

- examining the security documentation for the management of cyber security incidents as well as assessing the documentation's compliance with the PSPF and relevant ASD Cyber Security Guidelines;
- meeting with key staff responsible for protective security; cyber security; security incident management; security maturity monitoring; security planning and risk management; and reporting on security;
- conducting sample testing of responses to a cyber security incident, and recovery processes to determine if they were managed in accordance with the PSPF and relevant ASD Cyber Security Guidelines;
- undertaking walkthroughs of cyber security incident management response and recovery processes and gaining an understanding of the controls in place including the operational processes related to business continuity, disaster recovery, backup management and any lessons-learned exercises; and
- analysing the self-assessed ASD annual cyber security survey and the self-assessed PSPF annual security reporting submitted by AUSTRAC and Services Australia from 2017–18 to 2022–23.

1.33 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of approximately \$772,926.

1.34 The team members for this audit were Elijah Phal, Joanna Giang, Stevan Serafimov, Kelvin Le, Jason Ralston, Jade J. Koay, Sam Khaw, Edwin Apoderado, Xiaoyan Lu and Lesa Craswell.

2. Australian Transaction Reports and Analysis Centre's cyber security incident management

Areas examined

This chapter examined whether the Australian Transaction Reports and Analysis Centre (AUSTRAC) has appropriately designed and implemented cyber security incident management procedures for investigating, responding to, monitoring, reporting and recovering from cyber security incidents under the Protective Security Policy Framework (PSPF)⁴⁵ and relevant Australian Signals Directorate (ASD) Cyber Security Guidelines.⁴⁶

Conclusion

AUSTRAC has partly effective cyber security incident management procedures for investigating, monitoring and responding to cyber security incidents. It has established management structures and responsibilities as well as a framework of procedures for cyber security risk and incident management procedures to support these processes. It has not documented:

- the assigned responsibilities for its Chief Information Security Officer (CISO), although the CISO is empowered to make decisions;
- its approach to continuous monitoring and improvement reporting; or
- defined timeframes for reporting to stakeholders.

AUSTRAC has partly implemented effective response processes that mitigate disruptions during and after cyber security incidents. It has established a Security Information and Event Management (SIEM) solution and reporting processes for reporting significant or reportable cyber security incidents. The coverage of event logs is not in accordance with ASD's Cyber Security Guidelines. It does not have an event logging policy and does not document its analysis of all cyber security events.

AUSTRAC has documented procedures to support its cyber security incident recovery processes. These procedures do not include the security and testing of backup solutions, nor detail the systems, applications and servers supporting critical business processes. It performs recovery of backups as part of business area requests. It does not perform testing of restoration of backups for disaster recovery purposes.

Areas for improvement

The Australian National Audit Office (ANAO) made nine recommendations for AUSTRAC aimed at improving: the continuous assessment of risk in the security environment; reporting of cyber security risk to relevant stakeholders; management, documentation and maintenance of evidence; management and containment of cyber security incidents; implementation of SIEM solutions; monitoring, analysis and reporting of cyber security events; effectiveness of backups and recovery processes; integrity and resilience of data centres; and incorporation of post-incident lessons.

45 Department of Home Affairs, 'Protective Security Policy Framework' webpage, Home Affairs, Canberra, available from <https://www.protectivesecurity.gov.au> [accessed 9 April 2024].

46 Australian Signals Directorate, 'Cyber Security Guidelines' webpage, ASD, Canberra, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines> [accessed 9 April 2024].

2.1 AUSTRAC operates in an environment shaped by new and emerging technologies as well as criminals who become more sophisticated and develop new ways to exploit vulnerabilities in Australia's financial system.⁴⁷

2.2 Having effectively implemented arrangements for the management of cyber security incidents to deliver financial intelligence services such as Australia's anti-money laundering and counter-terrorism financing (AML/CTF) regulator and Financial Intelligence Unit (FIU) is important to the success of AUSTRAC's operations.

2.3 The PSPF specifies the requirements for how non-corporate Commonwealth entities such as AUSTRAC must apply the requirements outlined across the following PSPF policies:

- Policy 2 — Management structures and responsibilities;
- Policy 4 — Security maturity monitoring;
- Policy 5 — Reporting on security; and
- Policy 10 — Safeguarding data from cyber threats.⁴⁸

2.4 Supporting the PSPF are the relevant ASD Cyber Security Guidelines within the *Information Security Manual*⁴⁹, and ASD's *Essential Eight Maturity Model*.⁵⁰ As noted in paragraph 1.12, all NCEs that must apply the PSPF are required to self-assess and report on their level of maturity against four protective security outcomes.⁵¹

2.5 In this context, the ANAO examined whether AUSTRAC's:

- cyber security procedures supporting the planning for, managing, monitoring and reporting on, cyber security incidents were appropriately designed and implemented in accordance with the PSPF policies and the relevant ASD Cyber Security Guidelines;
- cyber security processes for investigating, monitoring and responding to cyber security incidents were implemented in accordance with the PSPF policies and the relevant ASD Cyber Security Guidelines; and

47 AUSTRAC, 'About Us' webpage, AUSTRAC, Canberra, 2024, available from <https://www.austrac.gov.au/about-us/what-we-do> [accessed 9 April 2024].

48 Department of Home Affairs, 'Applying the Protective Security Policy' webpage, Home Affairs, Canberra, available from <https://www.protectivesecurity.gov.au/about/applying-protective-security-policy-framework> [accessed on 9 April 2024].

49 Australian Signals Directorate, *Information Security Manual*, ASD, Canberra, March 2024, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism> [accessed on 8 April 2024]. Relevant guidelines are the *Guidelines for Cyber Security Incidents* available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents> [accessed on 8 April 2024], pp. 11–15; *Guidelines for Cyber Security Roles*, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-roles> [accessed on 8 April 2024], pp. 7–10; and *Guidelines for System Monitoring*, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-monitoring> [accessed on 8 April 2024], pp. 103–104.

50 Australian Signals Directorate, 'Essential Eight Maturity Model' webpage, ASD, Canberra, June 2017 (last updated November 2023), available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model> [accessed on 8 April 2024].

51 As noted in paragraph 1.10, this audit report will refer to the NCE entities that must apply the PSPF as 'entities', as is also used in the PSPF and supporting PSPF guidance.

- cyber security processes for recovery that mitigate disruptions to business operations during and after cyber security incidents were implemented and continuously improved.

Does AUSTRAC have appropriately designed and implemented cyber security incident management procedures?

AUSTRAC has established management structures and responsibilities for managing cyber security incidents. However, it has not documented the assigned responsibilities for its CISO although the CISO is empowered to make decisions.

AUSTRAC has documented a framework of procedures for cyber security risk and incident management. However, it does not detail a process for reviewing, updating and testing its cyber security incident management procedures, nor has it implemented a security maturity monitoring plan that details an approach that defines a continuous improvement cycle as well as reporting to management.

AUSTRAC has developed reporting processes for significant or reportable cyber security incidents.

AUSTRAC does not document cyber security incident meetings, nor has it defined timeframes for reporting to relevant stakeholders.

2.6 The appropriate design and implementation of cyber security incident management procedures is important in the effective implementation of arrangements for the management of cyber security incidents.

2.7 The PSPF Policies 2, 4 and 5 require that entities:

- implement assigned responsibilities for its appointed security roles;
- assess the cyber security risks within their security environments;
- meet external reporting obligations within required timeframes to the portfolio minister, the Department of Home Affairs (Home Affairs), other affected entities and ASD on cyber security matters; and
- appropriately design and implement cyber security incident management procedures in line with their assessed risk levels.

2.8 ASD's *Guidelines for Cyber Security Incidents* specify that cyber security incident management practices are likely to be more effective when they are well documented, embedded into daily operations and supported by senior management. The guidelines recommend:

- the design and implementation of a cyber security incident management policy;
- effective reporting of cyber security incidents to ASD and other affected entities that could be affected by unmitigated cyber security risks, incidents or vulnerabilities; and
- implementation of a trusted insider program.

2.9 As outlined in paragraph 1.29, AUSTRAC self-assessed its maturity level as Full for PSPF Policies 2 and 5 and Substantial for PSPF Policy 4 across 2022–23.

2.10 AUSTRAC's self-assessment against the PSPF Maturity Self-Assessment Model⁵² is set out in Table 2.1.

Table 2.1: AUSTRAC's reported maturity level against the PSPF Maturity Self-Assessment Model




PSPF Policy	Reported Maturity Level	Description of actions and controls
Policy 2 — Management structures and responsibilities	Three	The Chief Security Officer (CSO) is empowered to investigate, respond to and report on security incidents. Clearly defined security roles and responsibilities exist with skilled personnel appointed by the CSO and empowered to make security decisions for their entity. A governance oversight function is established (where appropriate to entity size). An entity's cycle of action, evaluation and learning is evident in response to security incidents. Personnel understand security incident reporting obligations with reporting processes published and accessible. Security is integral to the entity's business and informs decision-making. Leadership is actively engaged and visibly prioritises good security practices with a strong security culture evident within the entity. Personnel's participation in regular education programs that inform and assist their understanding of security-related processes and obligations is monitored.
Policy 4 — Security maturity monitoring	Two	Security capability and risk culture is broadly addressed in the security plan. The performance and progress against the security plan's goals and strategic objectives is substantially monitored regularly.
Policy 5 — Reporting on security	Three	The entity meets all external reporting obligations within required timeframes to the Portfolio Minister, Home Affairs, other affected entities and ASD on cyber security matters. The entity meets these obligations through effective reporting on achievement of security outcomes, implementation of core requirements, maturity of security capability, key risks to people, information and personnel and mitigation strategies. Key findings and trends are shared within the entity.

Source: ANAO analysis of AUSTRAC's self-reporting against the PSPF Maturity Self-Assessment Model.

2.11 The compliance of AUSTRAC's security plans, documentation and evidence of its implementation of PSPF Policies 2, 4, 5 and ASD's *Guidelines for Cyber Security Incidents* is summarised in Tables 2.2 to 2.5. Of the 13 requirements, two were fully implemented, nine were partly implemented, and two were not implemented.

52 Department of Home Affairs, *Protective Security Policy Framework – Assessment Report 2022–23*, Home Affairs, Canberra, 2023, available from <https://www.protectivesecurity.gov.au/system/files/2024-01/pspf-assessment-report-2022-23.pdf> [accessed on 8 April 2024], p. 4.

Table 2.2: AUSTRAC’s implementation of PSPF Policy 2 — Management structures and responsibilities

PSPF Policy 2 requirements	ANAO assessment	ANAO comment
<p>The accountable authority must:</p> <p>a) appoint a CSO at the Senior Executive Service level with a minimum security clearance of Negative Vetting Level 1, to be responsible for protective security in the [NCE]</p> <p>b) empower the CSO to make decisions about:</p> <p>... iv. investigating, responding to, and reporting on security incidents (other than cyber incidents)</p> <p>c) appoint a CISO with appropriate capability and experience and a minimum security clearance of Negative Vetting Level 1, to be responsible for cyber security in the entity</p> <p>d) empower the CISO to make decisions about:</p> <p>... v. investigating, responding to, and reporting on cyber incidents.</p>		<p>AUSTRAC has appointed the following cyber security roles with minimum security clearances of Negative Vetting Level 1:</p> <ul style="list-style-type: none"> • CSO; • Chief Information Security Officer (CISO); and • IT Security Advisor (ITSA). <p>AUSTRAC has designed and implemented assigned responsibilities for its CSO including empowering the CSO to make decisions.</p> <p>AUSTRAC has not documented the assigned responsibilities for its CISO, although the CISO is empowered to make decisions.</p>
<p>The CSO must be responsible for directing all areas of security to protect the entity’s people, information and assets. This includes appointing security advisors to support them in the day-to-day delivery of protective security and, to perform specialist services.</p>		<p>AUSTRAC has designed and implemented assigned responsibilities for its CSO including empowering the CSO to direct all areas of security to protect its people, information and assets.</p> <p>AUSTRAC has not established critical information and assets registers.</p>
<p>The CISO must be responsible for the entity’s cyber security program and associated implementation program. This includes appointing cyber security advisors to support them in the day-to-day delivery of cyber security, and to perform specialist services.</p>		<p>The CISO is not responsible for the cyber security program and associated implementation program. This responsibility has been assigned to the CSO.</p>

PSPF Policy 2 requirements	ANAO assessment	ANAO comment
<p>Entities must develop and use procedures that ensure:</p> <p>a) all elements of the entity's security plan are achieved;</p> <p>b) security incidents are investigated, responded to, and reported; and</p> <p>c) relevant security policy or legislative obligations are met.</p>	▲	<p>AUSTRAC has designed and implemented a framework of procedures for cyber security incident management that ensure relevant security policy or legislative obligations are met.</p> <p>AUSTRAC has not reviewed, updated and tested its Agency Security Plan and it does not have a documented plan to do so.</p> <p>AUSTRAC's CISO and ITSA regularly meet to discuss cyber security incidents. For significant or reportable cyber security incidents, the ITSA discusses these incidents with the CISO at the time of occurrence. These ad hoc meetings are not documented and are not supported by documented procedures.</p>
<p>A process of continual improvement be applied to monitoring, evaluating, responding to and managing security incidents.</p>	■	<p>AUSTRAC has not designed and implemented a security maturity monitoring plan that defines a continuous improvement cycle.</p>

Key: ◆ Fully implemented ▲ Partly implemented ■ Not implemented

Source: ANAO analysis of AUSTRAC's implementation of *PSPF Policy 2 — Management structures and responsibilities*.

Table 2.3: AUSTRAC's implementation of PSPF Policy 4 — Security Maturity Monitoring

PSPF Policy 4 requirements	ANAO assessment	ANAO comment
<p>Entities must assess the maturity of their security capability and risk culture by considering their progress against the goals and strategic objectives identified in their security plan.</p>	▲	<p>AUSTRAC annually submits its PSPF self-assessment report and its responses to the ASD cyber security survey.</p> <p>AUSTRAC does not have a security maturity monitoring plan which sets out the goals and strategic objectives identified in the Agency Security Plan and defines a continuous improvement cycle.</p>
<p>Entities document and evidence their assessment of their security maturity.</p>	▲	<p>AUSTRAC's PSPF self-assessment report specifies the results of the annual assessment of its security maturity.</p> <p>AUSTRAC does not regularly review, update, test and evidence the assessment of its security maturity.</p>
<p>Entities must maintain a monitored email address as the central conduit for all security-related matters across governance, personnel, information, cyber and physical security.</p>	▲	<p>AUSTRAC monitors a central email address, but has not documented its approach for triaging and responding to cyber security related matters using a monitored email address as the central conduit.</p>

Key: Fully implemented Partly implemented Not implemented

Source: ANAO analysis of AUSTRAC's implementation of *PSPF Policy 4 — Security Maturity Monitoring*.

Table 2.4: AUSTRAC's implementation of *PSPF Policy 5 — Reporting on Security*



PSPF Policy 5 requirements	ANAO assessment	ANAO comment
<p>Each entity must report:</p> <p>a) on security each financial year to its portfolio minister and the Department of Home Affairs ...</p> <p>b) on security to affected entities whose interests or security arrangements could be affected by the outcome of unmitigated security risks, security incidents or vulnerabilities in PSPF implementation</p> <p>c) on security to the Australian Signals Directorate in relation to cyber security matters ...</p> <p>d) any significant or reportable security incidents at the time they occur to:</p> <ul style="list-style-type: none"> the relevant authority; other affected entities; and the Department of Home Affairs. 		<p>AUSTRAC has submitted and completed the 2022–23 PSPF report on security and ASD's annual cyber security survey.</p> <p>AUSTRAC has implemented a process for reporting cyber security matters to ASD. Reporting timeframes have not been defined.</p> <p>AUSTRAC has not documented its approach or defined reporting timeframes for the reporting significant or reportable cyber security incidents to:</p> <ul style="list-style-type: none"> affected entities; and the process for how the Department of Home Affairs, as the owner of the PSPF, will be notified.
<p>Each entity must:</p> <p>a) submit a report on security each financial year; and</p> <p>b) complete the Australian Signals Directorate's annual cyber security survey.</p>		<p>AUSTRAC has submitted and completed the 2022–23 PSPF report on security and ASD's annual cyber security survey.</p>

Key: Fully implemented Partly implemented Not implemented

Source: ANAO analysis of AUSTRAC's implementation of *PSPF Policy 5 — Reporting on Security*.

Table 2.5: AUSTRAC's implementation of ASD's *Guidelines for Cyber Security Incidents*

Guideline recommendations	ANAO assessment	ANAO comment
<p>A cyber security incident management policy, and associated incident response plan, is developed, implemented and maintained.</p> <p>The cyber security incident management policy, including the associated cyber security incident response plan, is exercised at least annually.</p>		<p>AUSTRAC has designed and implemented a Protective Security Governance Policy as part of its cyber security incident management framework.</p> <p>AUSTRAC has not reviewed, updated or tested its Protective Security Governance Policy at least annually and does not have documented plans to do so.</p>

Guideline recommendations	ANAO assessment	ANAO comment
<p>Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.</p> <p>The types of cyber security incidents that should be reported to ASD include:</p> <ul style="list-style-type: none"> a) suspicious activities, such as privileged account lockouts and unusual remote access activities; b) compromise of sensitive or classified data; c) unauthorised access or attempts to access a system; d) emails with suspicious attachments or links; e) denial-of-service attacks; and f) ransomware attacks. <p>A cyber security incident register is developed, implemented and maintained.</p>		<p>AUSTRAC has implemented a process for reporting cyber security matters or incidents to ASD but not defined reporting timeframes.</p> <p>AUSTRAC does have a cyber security incident register.</p>
<p>A trusted insider program is developed, implemented and maintained.</p> <p>Legal advice is sought regarding the development and implementation of a trusted insider program.</p>		<p>AUSTRAC has developed, implemented and maintained an Insider Threat Management Framework. This framework was developed, implemented and maintained based on advice provided by relevant external entities and internal functions within AUSTRAC.</p>

Key:  Fully implemented  Partly implemented  Not implemented

Source: ANAO analysis of AUSTRAC's implementation of ASD's *Guidelines for Cyber Security Incidents*.

Management structures and responsibilities

2.12 In AUSTRAC, the Deputy Chief Executive Officer who is the Chief Operating Officer undertakes the CSO role. The Chief Information Officer undertakes the CISO role.

2.13 AUSTRAC has designed and implemented assigned responsibilities for the accountable authority and CSO. It has not designed and implemented assigned responsibilities for the CISO other than to say that 'the CSO can appoint senior executive service level security executives to support in the delivery of selected responsibilities'.

2.14 AUSTRAC has established a security sub-committee. The security sub-committee is chaired by the CSO and is responsible for the process of triaging security related risks, threats and associated responses. The management of cyber security risk and cyber security incident, including reviewing, updating and testing AUSTRAC's security documentation relies on the expertise of the ITSA and a small number of security advisors.

Cyber security risk management

2.15 AUSTRAC has designed and implemented registers, policies, plans and frameworks covering:

- cyber security risks;

- cyber security incident response and management; and
- information technology security and information security considerations.

2.16 AUSTRAC has not documented its approach to cyber security threat and vulnerability assessments and has not established critical information and asset registers. It has developed, implemented and maintained an Insider Threat Management Framework which is its trusted insider program. This framework was developed, implemented and maintained based on material and advice provided by relevant external entities and internal functions within AUSTRAC.

2.17 The majority of AUSTRAC's security documentation was last updated between June 2022 and August 2023, including those covering incident and risk management. The remainder of the documents were last updated between November 2015 and June 2022 and cover incident response. AUSTRAC does not have a documented plan to review, update and test its security documentation.

Cyber security incident management

2.18 AUSTRAC's framework of procedures for cyber security incident management includes its:

- Agency Security Plan;
- Protective Security Governance Policy;
- Information Systems Security Incident Response Plan; and
- security incident register.

2.19 Within its Agency Security Plan, AUSTRAC indicates that it takes a biennial approach for policies and risk reviews as well as an annual approach for standard operating procedures and guidelines.

2.20 The framework of procedures for cyber security incident management details how security incidents are identified, monitored, investigated, responded to, and reported. AUSTRAC has documented guidance covering incident response, business continuity, privacy and security reporting. AUSTRAC references external standards; such as, the Australian Government Investigations Standard, within its documented guidance.

2.21 AUSTRAC has not reviewed, updated and tested and does not have documented plans to review, update or test the framework of procedures for cyber security incident management procedures.

2.22 Within the Protective Security Governance Policy, there is no documented approach for how triaging and responding is undertaken using a monitored email address as the central conduit. The policy only specifies the Security Sub-committee being responsible for triaging and responding to security related risks and issues.

Security maturity monitoring plan

2.23 AUSTRAC does not have a security maturity monitoring plan. Instead, AUSTRAC self-assesses its security maturity as part of annually submitting and completing its PSPF report on security. The results of the PSPF report on security are used to structure a work plan of remediation exercises for the forthcoming year. The infrequency of AUSTRAC's monitoring makes it difficult for AUSTRAC to

substantiate that it was actively engaged in ongoing monitoring, specifically against the goals and strategic objectives identified in its security plan.

Recommendation no. 1

2.24 Australian Transaction Reports and Analysis Centre develops and implements:

- (a) policies that define the responsibilities of the Chief Information Security Officer in accordance with the Protective Security Policy Framework requirements; and
- (b) a security maturity monitoring plan that defines a continuous improvement cycle as well as reporting to management, including documenting the determination of reporting frequency and escalation.

Australian Transaction Reports and Analysis Centre response: *Agreed.*

2.25 *Commenced. AUSTRAC is undertaking a scheduled review and update of AUSTRAC's Security Governance Policy. AUSTRAC will define in the Security Governance Policy the responsibilities of the CISO in accordance with PSPF requirements. In March 2024, AUSTRAC's Security Working Group endorsed a Security Maturity Monitoring Plan in accordance with PSPF Policy 4.*

Internal reporting process

2.26 AUSTRAC's CISO has regular meetings with its ITSA. These meetings are to inform the CISO about cyber security incidents that have occurred since the last meeting. For significant or reportable cyber security incidents⁵³, the ITSA discusses these incidents with the CISO at the time of occurrence. These ad hoc meetings are not documented and are not supported by documented procedures.

2.27 AUSTRAC's Security Sub-committee was formed in 2019 to support AUSTRAC's Governance Committee.⁵⁴ The sub-committee reviews and discusses security-related information, initiatives and incidents, including cyber security incidents. The Security Sub-committee meets monthly and is chaired by the CSO. Its membership consists of the CISO, physical security advisor, personnel security advisor and the ITSA, and other relevant business areas.

2.28 The CISO provides monthly updates to AUSTRAC's Governance Committee and at Audit and Risk Committee meetings. The monthly updates include the outcomes of lessons learned exercises. AUSTRAC relies on risk reviews that are undertaken as part of the risk and internal audit processes.

External reporting process

2.29 AUSTRAC has submitted its PSPF report on security as well as ASD's cyber security survey annually. AUSTRAC's approach to external reporting has not defined reporting timeframes for

53 Home Affairs defines a significant security incident as a 'deliberate, negligent or reckless action that leads, or could lead to, the loss, damage, compromise, corruption or disclosure of official resources. A significant security incident can have wide ranging and critical consequences for the entity and the Australian Government.' See Department of Home Affairs, 'Significant security incident reporting template' webpage, Home Affairs, Canberra, 2019, available from <https://www.protectivesecurity.gov.au/publications-library/significant-security-incident-reporting-template> [accessed 9 April 2024].

54 The Governance Committee oversees the day-to-day operations of AUSTRAC and serves as an escalation point for sub-committees working groups. It is chaired by the CEO, or the Acting CEO or other nominee of the CEO.

referring significant or reportable cyber security incidents to ASD, affected NCEs, affected sectors and jurisdictions, and other notifiable authorities as recommended by ASD's *Cyber Incident Response Plan*. The *Cyber Incident Response Plan* also recommends that external reporting include a process for how the Department of Home Affairs, as the owner of the PSPF, will be notified.⁵⁵

2.30 AUSTRAC demonstrated it did not have any significant or reportable cyber security incidents to report to ASD during the audit period, 1 July 2022 to 31 October 2023. However, AUSTRAC advised of a referred a cyber security issue it had detected in September 2023 to ASD for advice. This referral was sent by the ITSA, with the support of the CISO, and finalised within 15 days from the date of referral.

Recommendation no. 2

2.31 Australian Transaction Reports and Analysis Centre develops and implements:

- (a) processes for ensuring cyber security incident meetings are documented;
- (b) timeframes for reporting to relevant external stakeholders; and
- (c) processes that ensure regular risk reporting to its Portfolio Minister and the Department of Home Affairs.

Australian Transaction Reports and Analysis Centre response: *Agreed.*

2.32 AUSTRAC will update our *Information Security Incident Response Plan* to:

- *refer expressly to the need to document and retain records of incident meetings, including identifying a person responsible for ensuring this occurs*
- *identify timeframes for reporting to relevant external stakeholders*
- *identify processes to ensure regular risk reporting to the Attorney-General and Department of Home Affairs.*

55 Australian Signals Directorate, *Cyber Incident Response Plan Guidance*, ASD, Canberra, July 2022, available from https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf [accessed 8 April 2024], p. 19.

Has AUSTRAC effectively implemented cyber security incident management processes for investigating, monitoring and responding to cyber security incidents?

AUSTRAC has reporting processes for reporting significant or reportable cyber security incidents to internal and external stakeholders. These processes do not include the engagement of relevant expertise in other business areas, such as legal advisors, and do not ensure the integrity of evidence supporting cyber security investigations.

AUSTRAC has documented cyber security incident monitoring and response procedures. It has not developed an event log policy for handling and containing malicious code infections or intrusions, or containment actions in the event of a data spill.

AUSTRAC has implemented a Security Information and Event Management (SIEM) solution. Its coverage of event logs is not in accordance with ASD's Cyber Security Guidelines. It undertakes an analysis of event logs and escalates significant or reportable cyber security incidents to management and relevant external stakeholders. It does not record or document its analysis of non-significant cyber security events, nor has it defined timeframes for triage and escalation activities.

AUSTRAC is able to analyse data within its SIEM solution, it does not have a process for retrieving and analysing production and archived SIEM data.

2.33 The *Information Security Manual* notes that 'establishing a cyber security incident management policy can increase the likelihood of successfully planning for, detecting and responding to malicious activity'.⁵⁶

2.34 PSPF Policy 2 outlines the management structures and responsibilities for how entities can ensure the effective implementation of security practices for investigating and responding to cyber security incidents. The policy requires that assigned security roles, responsibilities and management structures are defined to enable⁵⁷:

- the coordination or reporting on cyber security;
- the supervision of cyber security incident response activities and crisis management;
- the improvement of business resilience and ensure the continued operation of critical business processes; and
- the alignment of cyber security posture with its business objectives and the PSPF.

56 Australian Signals Directorate, 'Guidelines for Cyber Security Incidents' webpage, ASD, Canberra, last updated 1 March 2024, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents> [accessed on 8 April 2024].

57 Department of Home Affairs, *Protective Security Policy Framework — 2 Management structures and responsibilities*, Home Affairs, Canberra, 2018, last updated 30 August 2023, available from <https://www.protectivesecurity.gov.au/system/files/2023-08/policy-02-management-structures-and-responsibilities.pdf> [accessed on 8 April 2024], p. 3.


2.35 ASD's *Guidelines for Cyber Security Incidents*⁵⁸ and *Guidelines for System Monitoring*⁵⁹ note that cyber security practices are likely to be more effective and achieve security outcomes when they are well documented, embedded into daily operations and supported by senior management. These guidelines recommend:

- the development of cyber security incident response plans that document an approach to data spills, malicious code infections and intrusions;
- the development of event logging policies;
- the implementation of a centralised event logging facility; and
- the establishment of security practices that ensure the integrity of evidence following a cyber security incident.

2.36 As outlined in paragraph 1.29, AUSTRAC self-assessed as Full for PSPF Policy 2 in 2022–23.

2.37 The compliance of AUSTRAC's security plans, documentation and evidence of its implementation of PSPF Policy 2 and ASD's *Guidelines for Cyber Security Incidents* and *Guidelines for System Monitoring* are summarised in Tables 2.6 to 2.8. Of the seven requirements, three were partly implemented and four were not implemented.

Table 2.6: AUSTRAC's implementation of PSPF Policy 2 — Management structures and responsibilities

PSPF Policy 2 requirements	ANAO assessment	ANAO comment
Entities must develop and use procedures that ensure: <ul style="list-style-type: none"> a) all elements of the entity's security plan are achieved; b) security incidents are investigated, responded to, and reported; and c) relevant security policy or legislative obligations are met. 		AUSTRAC has designed and implemented a framework of procedures for responding to cyber security incidents. AUSTRAC has not reviewed, updated and tested its framework of procedures and it does not have a documented plan to do so. AUSTRAC's CISO and ITSA regularly meet to discuss cyber security incidents. For significant or reportable cyber security incidents, the ITSA discusses these incidents with the CISO at the time of occurrence. These ad hoc meetings are not documented and are not supported by documented procedures.



Key:  Fully implemented  Partly implemented  Not implemented



Source: ANAO analysis of AUSTRAC's implementation of *PSPF Policy 2 — Management structures and responsibilities*.

58 Australian Signals Directorate, 'Guidelines for Cyber Security Incidents' webpage, ASD, Canberra, last updated 1 March 2024, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents> [accessed on 8 April 2024].

59 Australian Signals Directorate, 'Guidelines for System Monitoring' webpage, ASD, Canberra, last updated 1 December 2023, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-monitoring> [accessed on 8 April 2024].

Table 2.7: AUSTRAC's implementation of ASD's *Guidelines for Cyber Security Incidents*

Guideline recommendations	ANAO assessment	ANAO comment
<p>When a data spill occurs, data owners are advised and access to the data is restricted.</p>		<p>AUSTRAC has designed and implemented procedures for handling data spills. The procedures do not specify actions for restricting access to data, systems and networks in the event of a data spill. A plan of containment is determined on a case-by-case basis based on operational team discussions. AUSTRAC has not developed an inventory of important datasets and their associated owners.</p>
<p>When malicious code is detected, the following steps are taken to handle and contain malicious code infections:</p> <ul style="list-style-type: none"> a) the infected systems are isolated; b) all previously connected media used in the period leading up to the infection are scanned for signs of infection and isolated if necessary; c) antivirus software is used to remove the infection from infected systems and media; and d) if the infection cannot be reliably removed, systems are restored from a known good backup or rebuilt. 		<p>AUSTRAC does not have a documented approach for handling and containing malicious code infections that details the recommended steps.</p>

Guideline recommendations	ANAO assessment	ANAO comment
<p>When an intrusion is detected, the following steps are taken to handle and contain the intrusion:</p> <ul style="list-style-type: none"> a) Legal advice is sought before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence. b) System owners are consulted before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence. c) Planning and coordination of intrusion remediation activities are conducted on a separate system to that which has been compromised. d) To the extent possible, all intrusion remediation activities are conducted in a coordinated manner during the same planned outage. e) Following intrusion remediation activities, full network traffic is captured for at least seven days and analysed to determine whether the adversary has been successfully removed from the system. 		<p>AUSTRAC does not have a documented approach for handling and containing intrusions that details the recommended steps.</p>
<p>The integrity of evidence gathered during an investigation is maintained by investigators in the following way:</p> <ul style="list-style-type: none"> a) recording all of their actions; b) maintaining a proper chain of custody; and c) following all instructions provided by relevant law enforcement agencies. 		<p>AUSTRAC has documented its approach to cyber security investigations of compromised servers, end-user computers and mobile phones within its Information Systems Incident Response Plan. However, this plan does not specify how an investigator will gather evidence in the recommended way following a cyber security incident.</p> <p>AUSTRAC refers to the <i>Australian Government Investigations Standard</i> within its Protective Security Governance Policy as the guidance to be used by its investigators.</p>

Key:  Fully implemented  Partly implemented  Not implemented

Source: ANAO analysis of AUSTRAC's implementation of ASD's *Guidelines for Cyber Security Incidents*.

Table 2.8: AUSTRAC's implementation of ASD's *Guidelines for System Monitoring*

Guideline recommendations	ANAO assessment	ANAO comment
<p>A centralised event logging facility is implemented in the following way:</p> <ul style="list-style-type: none"> a) event logs are sent to the facility as soon as possible after they occur; b) event logs are protected from unauthorised modification and deletion; and c) an accurate time source is established and used consistently across systems to assist with identifying connections between events. 	■	<p>AUSTRAC has not implemented a centralised event logging facility approach. However, it uses several event logging facilities covering different systems. This decentralised approach has not been implemented in the recommended way.</p>
<p>Cyber security events are analysed in a timely manner to identify cyber security incidents.</p>	■	<p>AUSTRAC does not have a documented approach for analysing cyber security events in a timely manner.</p>

Key: ◆ Fully implemented ▲ Partly implemented ■ Not implemented

Source: ANAO analysis of AUSTRAC's implementation of ASD's *Guidelines for System Monitoring*.

Cyber security incident response procedures

2.38 AUSTRAC has a framework of procedures for cyber security incident management. This framework includes procedures for responding to cyber security incidents.

2.39 AUSTRAC has associated guidance for cyber security incident response purposes which includes its:

- Privacy Breach Reporting Standard Operating Procedure;
- Privacy Policy and Procedures; and
- Business Continuity Business Impact Assessment Matrix.

2.40 Although associated guidance exists, AUSTRAC's security documentation does not define:

- how cyber security incidents are prioritised and, based on this prioritisation approach, how each cyber security incident will be managed and who coordinates or refers the response other than the ITSA or delegate triaging them;
- when, in terms of timeframes, are cyber security incidents should be referred from the ITSA to the CISO or from the CISO to the CSO;
- when communications relating to cyber security incidents are moved to, or recorded in, AUSTRAC's record-keeping repository after a cyber security incident has finalised;
- when to seek advice from other relevant business areas, such as digital forensic professionals, legal or law enforcement; and
- how the principles of maintaining the integrity of evidence would be observed during a cyber security investigation.

Recommendation no. 3

2.41 Australian Transaction Reports and Analysis Centre develops and implements:

- (a) procedures that define assigned security roles and responsibilities for coordinating responses, including engagement of relevant expertise; and
- (b) processes for managing and maintaining evidence during and after cyber security investigations.

Australian Transaction Reports and Analysis Centre response: *Agreed.*

2.42 *Commenced. AUSTRAC is undertaking a scheduled review of AUSTRAC's Security Governance Policy and will define the role of the CISO in the Policy. AUSTRAC's Information Security Incident Response Plan will be reviewed and updated to identify and define all roles and responsibilities relevant to coordinating responses to cybersecurity incidents and manage records of incidents. AUSTRAC will document evidence management during and after cyber security incident investigations in accordance with ISM guidelines.*

Management of data spills and malicious code

2.43 In May 2019, AUSTRAC designed and implemented an approach for handling data spills (which may also be referred to as a 'data breach' or a 'data leak'⁶⁰) within the Privacy Breach Reporting Standard Operating Procedure. Data spills are managed by the Privacy and Information Access Team (PIAT) using the Privacy Policy and Procedures and the Privacy Breach Reporting Standard Operating Procedure. Staff are required to report privacy breaches⁶¹ to the PIAT as soon as possible for containment and remediation.

2.44 An approach for containing data spills within its Privacy Breach Reporting Standard Operating Procedure has not been documented. The procedure does not specify actions for restricting access to data, systems and networks in the event of a data spill. A plan of containment is determined on a case-by-case basis based on operational team discussions.

2.45 A data inventory outlining important datasets and associated owners has not been developed by AUSTRAC. A project to establish a data inventory with an expected completion date of November 2024 is currently being undertaken.

2.46 AUSTRAC does not have an event log policy for handling and containing malicious code infections or intrusions. AUSTRAC relies on generic response plans outlined in the Information Systems Security Incident Response Plan. Specific response plans are determined on a case-by-case basis.

60 Australian Signals Directorate, *Data Spill Management Guide*, ASD, Canberra, 2012 (last updated October 2021), available from https://www.cyber.gov.au/sites/default/files/2023-04/protect_-_data_spill_management_guide_october_2021.pdf [accessed 8 April 2024].

61 AUSTRAC defines a 'privacy breach' as a breach against the *Privacy Act 1988*, which may include a notifiable data breach.

Recommendation no. 4

2.47 Australian Transaction Reports and Analysis Centre develops and implements:

- (a) an approach for containment actions that restrict access to data, systems and networks in the event of a data spill; and
- (b) an event log policy for handling and containing malicious code infections or intrusions.

Australian Transaction Reports and Analysis Centre response: *Agreed.*

2.48 *AUSTRAC's Information Security Incident Response Plan will be amended to reflect ISM guidelines regarding containment actions from data spills and event log handling to define relevant roles, processes, and record management.*

Management of remediation activities

2.49 The Information Security Policy specifies that the ITSA is responsible for implementing and managing information security arrangements, including being the Incident Manager during cyber security incidents. The ITSA is responsible for ensuring that the Information Systems Security Incident Response Plan is implemented; information is restored; and stakeholders are engaged. The Business Continuity RACI Matrix⁶² outlines assigned security roles and responsibilities during the business continuity process.

2.50 AUSTRAC has a Business Continuity Business Impact Assessment Matrix that specifies the criticality of ICT resources against specific business processes. The higher the criticality of the ICT resource against a business process, the greater the impact of the ICT resource has on the business process during a disruption event. AUSTRAC has not documented the use of the Business Continuity Business Impact Assessment Matrix during remediation activities.

2.51 AUSTRAC has documented its approach to incident investigations of compromised servers, end-user computers and mobile phones within its Information Systems Incident Response Plan. This plan does not specify how an investigator will gather evidence in the recommended way following a cyber security incident. AUSTRAC refers to the Australian Government Investigations Standard within its Protective Security Governance Policy as the guidance to be used by its investigators.

2.52 AUSTRAC plans and coordinates remediation and investigation activities via alternative communication channels. The use of a separate system enables AUSTRAC to continue with remediation activities outside of the compromised system. The CSO has directed staff to use specific products as approved alternative communication channels outside of the official network.

2.53 In addition, AUSTRAC has the ability to capture network traffic for the purposes of remediation and investigation activities. There is no documented event log retention policy which requires retrievable event logs for investigation purposes.

⁶² The acronym RACI stands for 'responsible, accountable, consulted and informed' and is a linear responsibility chart.

Security Information and Event Management solution

2.54 AUSTRAC has a Security Information and Event Management (SIEM) solution⁶³ in place to analyse cyber security events and has implemented a decentralised event logging approach.

2.55 The decentralised event logging approach was a result of historical management arrangements, where IT environments were managed by different AUSTRAC business areas and it has not been implemented in the recommended way (see Table 2.8). A centralised logging approach offers better control, efficiency and standardisation as recommended by the ASD's *Guidelines for System Monitoring*.⁶⁴ The management of the decentralised event logging approach is the responsibility of the ITSA.

2.56 AUSTRAC has not implemented ASD's recommendation for appropriate SIEM coverage or documented a strategy for prioritising its event monitoring resources due to a 'focus on implementing preventative controls to mitigate cyber security incidents'.

Recommendation no. 5

2.57 Australian Transaction Reports and Analysis Centre implements a strategy for Security Information and Event Management (SIEM) solution coverage that is in accordance with ASD's *Guidelines for System Monitoring* and performs a risk assessment to support any deviations from the guideline's recommendations.

Australian Transaction Reports and Analysis Centre response: *Agreed.*

2.58 *AUSTRAC will review its current SIEM coverage, which through three streams provides broad coverage over AUSTRAC's systems. AUSTRAC will investigate options for further centralisation of the SIEM. Should technical capability or resourcing limit the options for full centralisation, AUSTRAC will perform and document a risk assessment to support any differences with the ASD Guidelines for System Monitoring.*

Monitoring, analysis and reporting of cyber security events

2.59 Security alerts are configured within the SIEM solution and the SIEM solution allows for the automated assignment of priority to assist with triaging activities. AUSTRAC does not use this feature and security alerts are manually handled with the same level of priority. Security analysts monitor SIEM solution dashboards and perform ad hoc analysis of event logs. Any suspicious events are identified, triaged and escalated based on the expertise of the security analyst and under the guidance of the ITSA. Escalation discussions between security analysts and the ITSA occur verbally and are not documented. The ITSA informs the CISO of cyber security incidents during their weekly meetings. If the cyber security incident is significant, the ITSA informs the CISO at the time of cyber incident occurrence.

63 A Security Information and Event Management solution enables administrators to analyse event logs to help determine what activities are being performed within a network or system.

64 Australian Signals Directorate, 'Guidelines for System Monitoring' webpage, ASD, Canberra, last updated 1 December 2023, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-monitoring> [accessed 8 April 2024].

2.60 AUSTRAC's Information Systems Security Incident Response Plan states that 'all information must be saved for future analysis preferably to a location not itself susceptible to [a security] incident.'

2.61 Only significant SIEM investigations are reported and logged in AUSTRAC's record-keeping repository where 'significant' is defined by the security analyst. The SIEM investigation records include event logs, minutes and communications. Security alerts that have not been determined as 'significant' are only reported verbally.

2.62 AUSTRAC has not defined timeframes for analysing cyber security events, nor does it perform any analysis on the timeliness or completeness of triaging and escalation processes. AUSTRAC could not provide archived SIEM data from 1 June 2022 to 31 October 2023. AUSTRAC does not have processes for extracting and retrieving cyber security events from either the production environment or archives for future analysis.

Recommendation no. 6

2.63 Australian Transaction Reports and Analysis Centre establishes:

- (a) a process for retrieving and analysing production Security Information and Event Management (SIEM) solution data held within its SIEM solution and archived SIEM data;
- (b) record keeping requirements for triage and escalation activities over non-significant cyber security events to ensure completeness of activities; and
- (c) timeframe requirements for triage and escalation activities.

Australian Transaction Reports and Analysis Centre response: *Agreed.*

2.64 *AUSTRAC will document its current processes for retrieving backup production data for SIEM re-ingestion to facilitate historical event and incident analysis. AUSTRAC will document in our Information Security Incident Response Plan triage and escalation activities for non-significant cyber security events and timeframes for triage and escalation activities.*

2.65 The ANAO reviewed a cyber security issue which AUSTRAC detected in September 2023 and referred to ASD for advice (see paragraph 2.30). During September 2023, AUSTRAC was performing maintenance work on external interfacing systems. The cyber security team identified a cyber security issue and reviewed the associated logs before escalating it to the ITSA. The cyber security issue was escalated to the ITSA and communicated to the CISO and deputy CIO on the same day. The affected systems were monitored and key stakeholders were kept informed throughout. AUSTRAC engaged ASD for assistance during its investigation. The investigation was summarised in a minute to the CEO. In late September 2023, ASD advised AUSTRAC of the outcome of its assessment and officially closed the investigation.

Has AUSTRAC effectively implemented recovery processes that mitigate disruptions during and after cyber security incidents?

AUSTRAC has documented procedures to support its cyber security incident recovery processes. These procedures do not include the security and testing of backup solutions, nor detail the systems, applications and servers supporting critical business processes.

AUSTRAC has not tested the recoverability of its systems and applications supporting critical business processes. It has not included all relevant systems, including the tools used for managing backups, within disaster recovery testing schedules and security policies. It is not well placed to ensure business continuity or disaster recovery in the event of a significant or reportable cyber security incident.

AUSTRAC has primary and secondary data centres to support its approach to regular backups.

AUSTRAC performs recovery of backups as part of business area requests. It does not perform testing of restoration of backups for disaster recovery purposes. It does not have a process for extracting and analysing production and archive backup data.

AUSTRAC's incident reports include post-incident learning and post-remediation analysis. These reports are not used to review or update existing cyber security recovery procedures, with potential improvements highlighted in these reports not being considered for incorporation into existing cyber security documentation.

2.66 The *Information Security Manual* notes that 'establishing a cyber security incident management policy can increase the likelihood of successfully planning for, detecting and responding to malicious activity'.⁶⁵ Such arrangements could mitigate disruption to business operations during and after cyber security incidents and enable entities to recover data as well as the systems, applications and servers supporting critical business processes.⁶⁶

2.67 The PSPF Policy 10 requires entities to implement regular backup processes.⁶⁷ PSPF Policy 2 outlines the required management structures and responsibilities for implementing Policy 10 requirements, coordinating cyber security incident recovery activities as well as implementing post-incident learning to improve cyber security incident management arrangements.⁶⁸

65 Australian Signals Directorate, 'Guidelines for Cyber Security Incidents' webpage, ASD, Canberra, last updated 1 March 2024, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents> [accessed on 8 April 2024].

66 *ibid.*

67 Department of Home Affairs, *Protective Security Policy Framework — 10 Safeguarding data from cyber threats*, Home Affairs, Canberra, 2018 (last updated 19 February 2024), available from <https://www.protectivesecurity.gov.au/system/files/2024-02/policy-10-safeguarding-data-from-cyber-threats.pdf> [accessed on 8 April 2024], p. 2 (item B.1.a.viii).

68 Department of Home Affairs, *Protective Security Policy Framework — 2 Management structures and responsibilities*, Home Affairs, Canberra, 2018 (last updated 30 August 2023), available from <https://www.protectivesecurity.gov.au/system/files/2023-08/policy-02-management-structures-and-responsibilities.pdf> [accessed on 8 April 2024], p. 3.

2.68 ASD's *Guidelines for Cyber Security Roles*⁶⁹, *Guidelines for Cyber Security Incidents*⁷⁰ and the *Essential Eight Maturity Model*⁷¹ specify how entities can effectively implement arrangements for cyber security incident response processes. These guidelines:

- highlight the importance of the CISO role for overseeing cyber security incident response activities and contributing to business continuity and disaster recovering planning;
- recommend how entities enact their cyber security incident response plans following the identification of a cyber security incident; and
- recommend how entities can implement the Essential Eight mitigation strategies.

2.69 The Essential Eight mitigation strategies are the most effective of 37 prioritised mitigation strategies outlined in ASD's *Strategies to Mitigate Cyber Security Incidents*.⁷² The essential mitigation strategy for recovering data and system availability is called 'Regular backups'.

2.70 As outlined in paragraph 1.29, AUSTRAC self-assessed as Full for PSPF Policies 2 and 10 in 2022–23.

2.71 The compliance of AUSTRAC's cyber security incident recovery documentation as well as evidence of its implementation of PSPF Policies 2 and 10 as well as ASD's *Guidelines for Cyber Security Roles*, *Guidelines for Cyber Security Incidents* and the *Essential Eight Maturity Model* are summarised in Tables 2.9 to 2.13. Of the nine requirements, two were implemented, three were partly implemented, and four were not implemented.

Table 2.9: AUSTRAC's implementation of PSPF Policy 2 — Management structures and responsibilities

PSPF Policy 2 requirements	ANAO assessment	ANAO comment
<p>Entities must develop and use procedures that ensure:</p> <p>a) all elements of the entity's security plan are achieved;</p> <p>b) security incidents are investigated, responded to, and reported; and</p> <p>c) relevant security policy or legislative obligations are met.</p>	▲	<p>AUSTRAC has designed and implemented a framework of procedures for recovering from cyber security incidents.</p> <p>AUSTRAC has not reviewed, updated and tested its Agency Security Plan and it does not have a documented plan to do so.</p> <p>AUSTRAC's CISO and ITSA regularly meet to discuss cyber security incidents. For significant or reportable cyber security incidents, the ITSA discusses</p>

69 Australian Signals Directorate, 'Guidelines for Cyber Security Roles' webpage, ASD, Canberra, last updated 1 March 2024, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-roles> [accessed on 8 April 2024].

70 Australian Signals Directorate, 'Guidelines for Cyber Security Incidents' webpage, ASD, Canberra, last updated 1 March 2024, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents> [accessed on 8 April 2024].

71 Australian Signals Directorate, 'Essential Eight Maturity Model' webpage, ASD, Canberra, June 2017 (last updated November 2023) available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model> [accessed 8 April 2024].

72 Australian Signals Directorate, 'Strategies to Mitigate Cyber Security Incidents' webpage, ASD, Canberra, February 2010 (last updated February 2017), available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents/strategies-mitigate-cyber-security-incidents> [accessed 8 April 2024].

PSPF Policy 2 requirements	ANAO assessment	ANAO comment
		these incidents with the CISO at the time of occurrence. These ad hoc meetings are not documented and are not supported by documented procedures.
A process of continual improvement be applied to monitoring, evaluating, responding to and managing security incidents.	■	AUSTRAC has not designed and implemented a security maturity monitoring plan that defines a continuous improvement cycle as well as reporting to management.
Entities identify, document and share learnings internally ... and externally, where appropriate.	■	AUSTRAC does not use incident reports to update its framework of procedures for cyber security incident management or share learnings internally and externally, where appropriate.

Key: ◆ Fully implemented ▲ Partly implemented ■ Not implemented

Source: ANAO analysis of AUSTRAC's implementation of *PSPF Policy 2 — Management structures and responsibilities*.

Table 2.10: AUSTRAC's implementation of PSPF Policy 10 — Safeguarding data from cyber threats

PSPF Policy 10 requirements	ANAO assessment	ANAO comment
Each entity must mitigate common cyber threats by implementing the following mitigation strategies from the <i>Strategies to Mitigate Cyber Security Incidents</i> : ... regular backups	▲	AUSTRAC has a regular backup solution in place. The approach does not specify the details of protection measures for backup media devices.

Key: ◆ Fully implemented ▲ Partly implemented ■ Not implemented

Source: ANAO analysis of AUSTRAC's implementation of *PSPF Policy 10 — Safeguarding data from cyber threats*.

Table 2.11: AUSTRAC's implementation of ASD's Guidelines for Cyber Security Roles

Guideline recommendations	ANAO assessment	ANAO comment
The CISO contributes to the development and maintenance of business continuity and disaster recovery plans for their organisation to ensure that business-critical services are supported appropriately in the event of a disaster.	■	AUSTRAC has not designed and implemented assigned responsibilities for its CISO; such as, contributing to the development and maintenance of business continuity and disaster recovery plans.

Key: ◆ Fully implemented ▲ Partly implemented ■ Not implemented

Source: ANAO analysis of AUSTRAC's implementation of ASD's *Guidelines for Cyber Security Roles*.

Table 2.12: AUSTRAC's implementation of ASD's *Guidelines for Cyber Security Incidents*

Guideline recommendations	ANAO assessment	ANAO comment
Following the identification of a cyber security incident, an organisation's incident response plan and business continuity is enacted.	◆	AUSTRAC's Crisis Response Plan enacts the Information Systems Security Incident Response Plan and Business Continuity Plan.

Key: ◆ Fully implemented ▲ Partly implemented ■ Not implemented

Source: ANAO analysis of AUSTRAC's implementation of ASD's *Guidelines for Cyber Security Incidents*.

Table 2.13: AUSTRAC's implementation of ASD's *Essential Eight Maturity Model*

Guidance recommendations	ANAO assessment	ANAO comment
Backups of important data, software and configuration settings are implemented in the recommended way: a) performed and retained with a frequency and retention timeframe in accordance with business continuity requirements; b) synchronised to enable restoration to a common point in time; and c) retained in a secure and resilient manner.	▲	AUSTRAC has a regular backup solution in place which is implemented in the recommended way. However, it has not identified the systems, applications and servers which support critical business processes.
Unprivileged and privileged accounts (excluding backup administrator accounts): a) cannot access backups belonging to other accounts; and b) are prevented from modifying and deleting backups.	◆	AUSTRAC has implemented security controls to ensure that regular backups are stored in a secure and resilient manner and access, modification and deletion of backups is restricted appropriately.
Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.	■	AUSTRAC's recovery processes are tested through the restoration of various backups as part of infrastructure and business area requests. These are not specifically performed regularly as part of disaster recovery exercises.

Key: ◆ Fully implemented ▲ Partly implemented ■ Not implemented

Source: ANAO analysis of AUSTRAC's implementation of ASD's *Essential Eight Maturity Model*.

Cyber security recovery procedures

2.72 As outlined at paragraph 2.18, AUSTRAC has a framework of procedures for cyber security incident management. This framework includes procedures for recovering from cyber security incidents.

2.73 AUSTRAC has associated guidance for cyber security incident recovery which includes:

- Business Continuity Plan;

- IT Disaster Recovery Strategy;
- Crisis Response Plan;
- Information Systems Security Incident Response Plan; and
- Privacy Breach Reporting Standard Operating Procedure.

2.74 As outlined at paragraph 2.21, AUSTRAC has not reviewed, updated and tested and does not have documented plans to review, update or test the framework of procedures for cyber security incident management.

2.75 The cyber security incident recovery process, including incident escalation, is outlined within the Business Continuity Plan. The disaster recovery process is specified in the IT Disaster Recovery Strategy. There is no mention of the application of any business impact analysis.⁷³ AUSTRAC advised the ANAO that the Information Systems Security Incident Response Plan and the Business Continuity Plan are required to be enacted as soon as the Crisis Response Plan has been enacted by AUSTRAC's Crisis Management Team.

2.76 The Information Systems Security Incident Response Plan outlines responsibilities, procedures, incident resolution, maximum allowable outages by critical business process, and AUSTRAC's approach to regular backups. The systems, applications and servers which support critical business processes, have not been identified. AUSTRAC only specifies the use of business continuity workarounds and alternate systems, equipment or facilities.

2.77 AUSTRAC's recovery documentation does not include:

- its regular backup solutions within the scope of AUSTRAC's security policies and disaster recovery testing schedule;
- the approach to prioritising encryption of regular backups; and
- details of protection measures for backup media devices.

73 AUSTRAC's cyber security incident recovery process is a six-step process covering IT disaster recovery directions; activity leads; activating business continuity workarounds and monitoring progress; deactivating business continuity workarounds; closing a business continuity event; and storage of disaster recovery documentation.

Recommendation no. 7

2.78 Australian Transaction Reports and Analysis Centre develops and implements:

- (a) disaster recovery testing schedules that include backup solutions;
- (b) business continuity planning processes that incorporate the systems, applications and servers which support critical business processes; and
- (c) processes that test the recoverability of its systems and applications supporting critical business processes, including implementing any lessons learned into future testing schedules.

Australian Transaction Reports and Analysis Centre response: *Agreed.*

2.79 *Commenced. AUSTRAC is finalising an update to its agency-wide business continuity plan, which includes components relevant to backup and recovery, such as timeframes, consultation and associated risks. AUSTRAC will develop testing schedules consistent with our risk profile and appetite and operational requirements.*

Performing and retaining regular backups

2.80 AUSTRAC has a regular backup solution in place that stores both production and archived backup data. AUSTRAC also has a backup solution to manage the regular backup of network devices. Additional software is deployed to each system to enable backup and recovery of transaction logs.⁷⁴ Full and incremental backups of related systems are restorable to a point in time.

2.81 Regular backup requirements are documented and set by the system owners as part of the System Security Plans. Regular backup requirements for some systems have not been documented.

2.82 Production data is hosted at AUSTRAC's primary data centre and backup data is located at a secondary data centre which have both been assessed by the Digital Transformation Agency as providing the highest level of security assurance under the Hosting Certification Framework.

Restricting access to backups

2.83 AUSTRAC has implemented security controls to ensure that regular backups are stored in a secure and resilient manner and access, modification and deletion of backups is restricted appropriately. For example, backup policies and processes comply with PROTECTED requirements as datasets are considered PROTECTED information.

2.84 Administrative account access to the regular backup solution is restricted. Administrative accounts can access their regular backups but cannot access the backups of any other administrative accounts.

2.85 Backup system administrators have access to all backups, with individual sub-system backup administrators having access to their own system's backups. Any user accounts, excluding backup system administrator accounts, are prevented from accessing, modifying and deleting backups. The backup system administrator may modify or delete backups but only after a four-week legal hold period from the point that the backups are taken.

74 System restore does not imply successful recovery of production data.

Regular testing of backups

2.86 AUSTRAC does not perform complete system disaster testing as part of disaster recovery exercises 'due to the size of its information holdings and budget allocation'. AUSTRAC does not have a process for extracting and analysing production and archived backup data. Recovery processes are tested through the restoration of various backups as part of infrastructure and business area requests. These are not specifically performed regularly as part of disaster recovery exercises. As such, AUSTRAC is not well placed to ensure business continuity or disaster recovery in the event of a significant or reportable cyber security incident.

2.87 AUSTRAC advised the ANAO that during the audit period it has not had a significant or reportable cyber security incident and consequently has not needed to recover backups in response to a cyber security incident.

Recommendation no. 8

2.88 Australian Transaction Reports and Analysis Centre establishes a program that assesses the effectiveness of recovery processes for all production and archived backup data.

Australian Transaction Reports and Analysis Centre response: *Agreed.*

2.89 *AUSTRAC will develop a program to assess the effectiveness of recovery processes for all production and archived backup data.*

Appropriately documented and embedded post-incident learning approach

2.90 AUSTRAC's incident reports include post-incident learning and post-remediation analysis. AUSTRAC undertook a root-cause analysis of the cyber security issue in 2023 which identified some systematic improvements. AUSTRAC does not use these incident reports to design and implement a security maturity monitoring plan or update its framework of procedures for cyber security incident management or share learnings internally and externally, where appropriate.⁷⁵

2.91 As outlined at paragraphs 2.21 and 2.23, AUSTRAC does not regularly review, update or test its security documentation and procedures and has not documented a security maturity monitoring plan.

75 Department of Home Affairs, *Protective Security Policy Framework – 2 Management structures and responsibilities*, Home Affairs, Canberra, 2018 (last updated 30 August 2023), available from <https://www.protectivesecurity.gov.au/system/files/2023-08/policy-02-management-structures-and-responsibilities.pdf> [accessed on 8 April 2024], Annex A-2.

Recommendation no. 9

2.92 Australian Transaction Reports and Analysis Centre leverage its post-incident learning approaches following a cyber security incident to inform a process that reviews, updates and tests all of the relevant security documentation for the effective management of cyber security incidents. That is:

- (a) supporting security documentation to its security plans;
- (b) framework of procedures for cyber security incident management;
- (c) associated guidance for cyber security incident response; and
- (d) associated guidance for cyber security incident recovery.

Australian Transaction Reports and Analysis Centre response: *Agreed.*

2.93 *AUSTRAC has a current process of conducting 'lessons learnt' exercises following an incident. AUSTRAC will document this process in AUSTRAC's Information Security Incident Response Plan and extend it to require lessons identified to be actioned through updates and tests of all relevant security documentation for managing cyber security incidents.*

3. Services Australia’s cyber security incident management

Areas examined

This chapter examined whether the Services Australia has appropriately designed and implemented cyber security incident management procedures for investigating, responding to, monitoring, reporting and recovering from cyber security incidents under the Protective Security Policy Framework (PSPF)⁷⁶ and relevant Australian Signals Directorate (ASD) Cyber Security Guidelines.⁷⁷

Conclusion

Services Australia is partly effective in its design of cyber security incident management procedures. It has established a framework of procedures and an incident response plan. It has not documented an approach to threat and vulnerability assessments. It does not have a policy covering the management of cyber security incidents.

Services Australia has partly effective cyber security incident response procedures for investigating and responding to cyber security incidents. It has procedures for managing data spills, malicious code infections and external instructions. It has implemented a Security Information and Event Management (SIEM) solution and a systematic approach to monitoring and prioritisation of alerts. Services Australia has not established a timeframe for triage and escalation activities nor a process for analysing archived SIEM data. It has not defined an approach for cyber security investigations.

Services Australia has partly implemented effective recovery processes to mitigate disruptions during and after cyber security incidents. It has developed business continuity and disaster recovery plans and implemented regular backups. Its plans do not include all systems and applications supporting critical business processes and it does not test the recoverability of backups.

Areas for improvement

The Australian National Audit Office (ANAO) made 10 recommendations aimed at: improving the continuous assessment of risk in the security environment; reporting of cyber security risk to relevant stakeholders; management, documentation and maintenance of evidence; monitoring, analysis and reporting of cyber security events; effectiveness of backups and recovery processes; as well as, incorporation of post-incident lessons.

3.1 Services Australia operates in an environment shaped by new and emerging technologies as well as the ‘events of recent years, including the Coronavirus disease (COVID-19) pandemic and a number of natural disasters and emergencies’ which has ‘transformed’ its business.⁷⁸

76 Department of Home Affairs, ‘Protective Security Policy Framework’ webpage, Home Affairs, Canberra, available from <https://www.protectivesecurity.gov.au> [accessed 9 April 2024].

77 Australian Signals Directorate, ‘Cyber Security Guidelines’ webpage, ASD, Canberra, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines> [accessed 9 April 2024].

78 Services Australia, *Corporate Plan 2023-24*, SA, available from <https://www.servicesaustralia.gov.au/sites/default/files/2023-08/corporate-plan-23-24.pdf> [accessed 20 March 2024], p. 6.

3.2 Having effectively implemented arrangements for the management of cyber security incidents in order to deliver essential social, health and welfare services to the Australian public is fundamental to the success of Services Australia's operations.

3.3 The PSPF specifies the requirements for how non-corporate Commonwealth entities such as Services Australia must apply the requirements outlined across the following PSPF policies:

- Policy 2 — Management structures and responsibilities;
- Policy 4 — Security maturity monitoring;
- Policy 5 — Reporting on security; and
- Policy 10 — Safeguarding data from cyber threats.⁷⁹

3.4 Supporting the PSPF are the relevant ASD Cyber Security Guidelines within the *Information Security Manual*⁸⁰, and ASD's *Essential Eight Maturity Model*.⁸¹ As noted in paragraph 1.12, all NCEs that must apply the PSPF are required to self-assess and report on their level of maturity against four protective security outcomes.⁸²

3.5 In this context, the ANAO examined whether Services Australia's:

- cyber security procedures supporting the planning for, managing, monitoring and reporting on, cyber security incidents were appropriately designed and implemented in accordance with the PSPF policies and the relevant ASD Cyber Security Guidelines;
- cyber security processes for investigating, monitoring and responding to cyber security incidents were implemented in accordance with the PSPF and the relevant ASD Cyber Security Guidelines; and
- cyber security processes for recovery that mitigate disruptions to business operations during and after cyber security incidents were implemented and continuously improved.

79 Department of Home Affairs, 'Applying the Protective Security Policy' webpage, Home Affairs, Canberra, available from <https://www.protectivesecurity.gov.au/about/applying-protective-security-policy-framework> [accessed on 9 April 2024].

80 Australian Signals Directorate, *Information Security Manual*, ASD, Canberra, March 2024 available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism> [accessed on 8 April 2024]. Relevant guidelines are the *Guidelines for Cyber Security Incidents* available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents> [accessed on 8 April 2024], pp. 11–15; *Guidelines for Cyber Security Roles* available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-roles> [accessed on 8 April 2024], pp. 7–10; and *Guidelines for System Monitoring* available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-monitoring> [accessed on 8 April 2024], pp. 103–104.

81 Australian Signals Directorate, 'Essential Eight Maturity Model' webpage, ASD, Canberra, June 2017 (last updated November 2023), available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model> [accessed 8 April 2024].

82 As noted in paragraph 1.10, this audit report will refer to the NCE entities that must apply the PSPF as 'entities', as is also used in the PSPF and supporting PSPF guidance.

Does Services Australia have appropriately designed and documented cyber security incident management procedures?

Services Australia has established management structures and responsibilities for its management of cyber security incidents. It has not documented an approach to threat and vulnerability assessments, nor does it have a policy covering the management of cyber security incidents. While Services Australia has a security maturity monitoring plan, this does not detail an approach that defines a continuous improvement cycle as well as reporting to management.

Services Australia has developed a cyber security incident response plan and a trusted insider program. However, its trusted insider program has not considered input from other business areas, such as its legal function. Services Australia's critical asset and data registers do not have complete information on critical systems and data assets.

Services Australia has documented a framework of procedures for cyber security risk and incident management. However, it does not detail a process for reviewing, updating and testing its cyber security incident management procedures.

Services Australia has reporting processes that provide regular reporting of cyber security incidents, including significant or reportable cyber security incidents, to internal and external stakeholders. It has not defined the timeframes for reporting to relevant stakeholders and the consideration of engaging other relevant expertise, such as legal advisors, during reporting processes.

3.6 The appropriate design and implementation of cyber security incident management procedures is important in the effective implementation of arrangements for the management of cyber security incidents.

3.7 PSPF Policies 2, 4 and 5 require that entities:

- implement assigned responsibilities for its appointed security roles;
- assess the cyber security risks within their security environments;
- meet external reporting obligations within required timeframes to the portfolio minister, Home Affairs, other affected entities and ASD on cyber security matters; and
- appropriately design and implement cyber security incident management procedures in line with their assessed risk levels.

3.8 ASD's *Guidelines for Cyber Security Incidents* specify that cyber security incident management practices are likely to be more effective when they are well documented, embedded into daily operations and supported by senior management. This guideline recommends:

- the design and implementation of a cyber security incident management policy;
- effective reporting of cyber security incidents to ASD and other affected entities that could be affected by unmitigated cyber security risks, incidents or vulnerabilities; and
- implementation of a trusted insider program.

3.9 As outlined in paragraph 1.29, Services Australia self-assessed as Substantial for PSPF Policies 2 and 4 and Full for PSPF Policy 5 in 2022–23.

3.10 Services Australia's self-assessment against the PSPF Self-Assessment Maturity Model is set out in Table 3.1.




Table 3.1: Services Australia's reported maturity level against the PSPF Self-Assessment Maturity Model



PSPF Policies	Maturity Level	Description of actions and controls
Policy 2	Substantial	The Chief Security Officer (CSO) is empowered to investigate, respond to and report on security incidents. Clearly defined security roles and responsibilities exist with skilled personnel appointed by the CSO and empowered to make security decisions for their entity. A governance oversight function is established (where appropriate to entity size). An entity's cycle of action, evaluation and learning is evident in response to security incidents. Personnel understand security incident reporting obligations with reporting processes published and accessible. Security is integral to the entity's business and informs decision-making. Leadership is actively engaged and visibly prioritises good security practices with a strong security culture evident within the entity. Personnel's participation in regular education programs that inform and assist their understanding of security-related processes and obligations is monitored.
Policy 4	Substantial	Security capability and risk culture is broadly addressed in the security plan. The performance and progress against the security plan's goals and strategic objectives is substantially monitored regularly.
Policy 5	Full	The entity meets all external reporting obligations within required timeframes to the Portfolio Minister, Home Affairs, other affected entities and ASD on cyber security matters. The entity meets these obligations through effective reporting on achievement of security outcomes, implementation of core requirements, maturity of security capability, key risks to people, information and personnel and mitigation strategies. Key findings and trends are shared within the entity.

Source: ANAO analysis of Services Australia's reporting against the PSPF Self-Assessment Maturity Model.

3.11 The compliance of Services Australia's security plans, documentation and evidence of its implementation of PSPF Policies 2, 4, 5 and ASD's *Guidelines for Cyber Security Incidents* is summarised in Tables 3.2 to 3.5. Of the 13 requirements, four were implemented, eight were partly implemented and one was not implemented.

Table 3.2: Services Australia’s implementation of PSPF Policy 2 — Management structures and responsibilities

PSPF Policy 2 requirements	ANAO assessment	ANAO comment
<p>The accountable authority must:</p> <p>a) appoint a CSO at the Senior Executive Service level with a minimum security clearance of Negative Vetting Level 1, to be responsible for protective security in the [NCE]</p> <p>b) empower the CSO to make decisions about:</p> <p>... iv. Investigating, responding to, and reporting on security incidents (other than cyber incidents).</p> <p>c) appoint a Chief Information Security Officer (CISO) with appropriate capability and experience and a minimum security clearance of Negative Vetting Level 1, to be responsible for cyber security in the entity</p> <p>d) empower the CISO to make decisions about:</p> <p>... v. investigating, responding to, and reporting on cyber incidents.</p>		<p>Services Australia has appointed the following cyber security roles with minimum security clearances of Negative Vetting Level 1:</p> <ul style="list-style-type: none"> • CSO; • Chief Information Security Officer (CISO); and • Information Technology Security Advisor (ITSA). <p>Services Australia has designed and implemented assigned responsibilities for its CSO and CISO including empowering the CSO and CISO to make decisions.</p>
<p>The CSO must be responsible for directing all areas of security to protect the entity’s people, information and assets. This includes appointing security advisors to support them in the day-to-day delivery of protective security and, to perform specialist services.</p>		<p>Services Australia has designed and implemented assigned responsibilities for its CSO including empowering the CSO to direct all areas of security to protect its people, information and assets.</p> <p>Services Australia has established critical information and assets registers. However, the registers are incomplete and do not specify all critical systems and data assets.</p>
<p>The CISO must be responsible for the entity’s cyber security program and associated implementation program. This includes appointing cyber security advisors to support them in the day-to-day delivery of cyber security, and to perform specialist services.</p>		<p>The CISO is responsible for the cyber security program and associated implementation program.</p>

PSPF Policy 2 requirements	ANAO assessment	ANAO comment
<p>Entities must develop and use procedures that ensure:</p> <ul style="list-style-type: none"> • all elements of the entity's security plan are achieved; • security incidents are investigated, responded to, and reported; and • relevant security policy or legislative obligations are met. 		<p>Services Australia has designed and implemented a framework of procedures for cyber security incident management that ensure relevant security policy or legislative obligations are met. This includes:</p> <ul style="list-style-type: none"> • Protective Security Plan 2023–25; • Cyber Security Incident Response Plan; and • Security Incident Register. <p>Services Australia has an Incident Management and Escalation Policy. However, Services Australia removed 'cyber security incidents' from the Incident Management and Escalation Policy in June 2023, and advised the ANAO in January 2024 that cyber security incidents are managed by the 'relevant business teams' within the Cyber Security Division.</p> <p>The majority of Services Australia's security documentation was last updated between June 2022 and December 2023. Services Australia does not have a documented plan to review, update and test its security documentation.</p> <p>Services Australia's CISO, with the support of national managers within the Cyber Security Division, is informed, through secure communication channels, about cyber security incidents which have been prioritised between the second and fourth levels.^a For more significant or reportable cyber security incidents which have been prioritised at the highest level, the CISO acts as the incident controller.</p>
<p>A process of continual improvement be applied to monitoring, evaluating, responding to and managing security incidents.</p>		<p>Services Australia has a security maturity monitoring plan called the Protective Security Risk Management Plan, although it has not defined a continuous improvement cycle as well as reporting to management.</p>

Key:  Fully implemented  Partly implemented  Not implemented

Note a: Services Australia's cyber security incident severity classifications are rated between 1 and 4, with 1 being the highest severity and 4 being the lowest.

Source: ANAO analysis of Services Australia's implementation of *PSPF Policy 2 — Management structures and responsibilities*.

Table 3.3: Services Australia’s implementation of PSPF Policy 4 — Security Maturity Monitoring


PSPF Policy 4 requirements	ANAO assessment	ANAO comment
Entities must assess the maturity of their security capability and risk culture by considering their progress against the goals and strategic objectives identified in their security plan.	▲	Services Australia submits its PSPF security report and its responses to the ASD cyber security survey annually. Services Australia has a security maturity monitoring plan called the Protective Security Risk Management Plan, although it has not defined a continuous improvement cycle as well as reporting to management.
Entities document and evidence their assessment of their security maturity.	▲	Services Australia has designed and implemented policies, plans and frameworks for cyber security incident management. Services Australia does not regularly review, update, test and evidence the assessment of its security maturity.
Entities must maintain a monitored email address as the central conduit for all security-related matters across governance, personnel, information, cyber and physical security.	■	Services Australia has documented its approach for triaging and responding to cyber security related matters. However, there is no monitored email address as the central conduit documented.

Key: ◆ Fully implemented ▲ Partly implemented ■ Not implemented

Source: ANAO analysis of Services Australia’s implementation of PSPF Policy 4 — Security Maturity Monitoring.

Table 3.4: Services Australia’s implementation of PSPF Policy 5 — Reporting on Security



PSPF Policy 5 requirements	ANAO assessment	ANAO comment
Each entity must report: <ol style="list-style-type: none"> a) on security each financial year to its Portfolio Minister and the Department of Home Affairs ... b) on security to affected entities whose interests or security arrangements could be affected by the outcome of unmitigated security risks, security incidents or vulnerabilities in PSPF implementation c) on security to the Australian Signals Directorate in relation to cyber security matters ... and d) any significant or reportable security incidents at the time they occur to: <ul style="list-style-type: none"> • the relevant authority ... • other affected entities; and 	▲	Services Australia has submitted and completed the 2022–23 PSPF report on security and ASD’s annual cyber security survey. Services Australia has implemented a process for reporting cyber security matters to ASD but not defined reporting timeframes. Services Australia has not documented its approach or defined reporting timeframes for the reporting significant or reportable cyber security incidents to: <ul style="list-style-type: none"> • affected entities; and • the process for how the Department of Home Affairs, as the owner of the PSPF, will be notified.

PSPF Policy 5 requirements	ANAO assessment	ANAO comment
<ul style="list-style-type: none"> the Department of Home Affairs. 		
<p>Each entity must:</p> <ol style="list-style-type: none"> submit a report on security each financial year ... and complete the Australian Signals Directorate's annual cyber security survey. 		<p>Services Australia has submitted and completed the 2022–23 PSPF report on security and ASD's annual cyber security survey.</p>

Key:  Fully implemented  Partly implemented  Not implemented.

Source: ANAO analysis of Services Australia's implementation of *PSPF Policy 5 — Reporting on Security*.

Table 3.5: Services Australia's implementation of ASD's *Guidelines for Cyber Security Incidents*

Guideline recommendations	ANAO assessment	ANAO comments
<p>A cyber security incident management policy, and associated incident response plan, is developed, implemented and maintained.</p> <p>The cyber security incident management policy, including the associated cyber security incident response plan, is exercised at least annually.</p>		<p>Services Australia has designed and implemented an Incident Management and Escalation Policy as part of its cyber security incident management framework. However, Services Australia removed 'cyber security incidents' from the Incident Management and Escalation Policy in June 2023, and advised the ANAO in January 2024 that cyber security incidents are managed by the 'relevant business teams' within the Cyber Security Division.</p> <p>Services Australia has designed and implemented a Cyber Security Incident Response Plan.</p> <p>Services Australia has not reviewed, updated or tested its Incident Management and Escalation Policy at least annually and does not have documented plans to do so.</p>
<p>Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.</p> <p>The types of cyber security incidents that should be reported to ASD include:</p> <ol style="list-style-type: none"> suspicious activities, such as privileged account lockouts and unusual remote access activities; compromise of sensitive or classified data; unauthorised access or attempts to access a system; emails with suspicious attachments or links; 		<p>Services Australia has implemented a process for reporting cyber security matters or incidents to ASD but not defined reporting timeframes.</p> <p>Services Australia does have a cyber security incident register which is called the security incident register.</p>

Guideline recommendations	ANAO assessment	ANAO comments
e) denial-of-service attacks; and f) ransomware attacks. A cyber security incident register is developed, implemented and maintained.		
A trusted insider program is developed, implemented and maintained. Legal advice is sought regarding the development and implementation of a trusted insider program.	▲	Services Australia has developed, implemented and maintained an Integrity Framework. This framework was developed, implemented and maintained without advice provided by relevant external entities and internal functions within Services Australia.

Key: ◆ Fully implemented ▲ Partly implemented ■ Not implemented

Source: ANAO analysis of Services Australia's implementation of ASD's *Guidelines for Cyber Security Incidents*.

Management structures and responsibilities

3.12 Services Australia has defined management structures for cyber security roles which includes a CSO, Deputy CSOs and a CISO.

3.13 The responsibilities for the accountable authority, CSO and Deputy CSOs and CISO include:

- governance consistent with Australian Government policies, including the PSPF;
- implementation of whole-of-government mandatory security directions;
- chairing of the Security Sub-Group by the Chief Executive Officer (CEO), with the support of the CSO; and
- the appointment of a CISO as well as cyber security personnel by the CSO to assist the CSO and accountable authority with the day-to-day delivery of security and specialist services.

3.14 The most senior governance committee in Services Australia is the Executive Committee, which is supported by the Security Committee. The CISO chairs the Cyber Resilience Board and the Strategic Cyber Security CISO Board. The membership and relevant security responsibilities of the Executive and Security Committees are summarised in Table 3.6.

Table 3.6: Services Australia's Executive and Security Committees

Governing body	Membership	Security responsibilities ^a
Executive Committee	<ul style="list-style-type: none"> • Chief Executive Officer (Chair); • All Deputy Chief Executive Officers; • Chief Counsel; • Chief Financial Officer; • General Manager Communications; and • General Manager Enterprise Strategy and Governance. 	<ul style="list-style-type: none"> • Oversees the entity's system of risk management; • Manages of enterprise risks; and • Resolves significant issues or matters escalated by other enterprise governance forums.

Governing body	Membership	Security responsibilities ^a
Security Committee	<ul style="list-style-type: none"> • Chief Operating Officer; • Chief Security Officer (Chair); • Chief Counsel; • Chief Data Officer; • General Manager Corporate and Cross Government Services (Deputy Chief Security Officer); • General Manager Cyber Security (Deputy Chief Security Officer and Chief Information Security Officer); • General Manager Face to Face Services; • General Manager Fraud Control and Investigations (Deputy Chief Security Officer); • General Manager Older Australians and Veterans; • General Manager People; and • General Manager Service Delivery Learning and Face to Face Transformation. 	<ul style="list-style-type: none"> • Supports the Executive Committee; • Provides a coordinated approach to security and associated risk across the entity; • Escalation point for risks relating to security, privacy, cyber security and data; • Considers the outcomes of security incidents and investigations; and • Considers the implementation of security controls.

Note a: Only includes the responsibilities relevant to cyber security risk and incident management.

Source: ANAO analysis of Services Australia's governance documentation.

3.15 The management of cyber security risk and cyber security incident, including reviewing, updating and testing Services Australia's security documentation relies on the expertise of the Cyber Security Division which is led by the CISO.

Cyber security risk management

3.16 Services Australia has documented policies, plans, frameworks covering:

- enterprise risk and risk management;
- cyber security incident response;
- cyber security governance;
- trusted insider program;
- an information asset register;
- playbooks that address several adversary tactics; and
- a Privacy Incident and Data Breach Response Plan.

3.17 Services Australia has not documented its approach to threat and vulnerability assessments. Services Australia has documented an Integrity Framework which is its trusted insider program. This framework does not include input on threats from other business areas such as legal functions.

Recommendation no. 10

3.18 Services Australia updates its trusted insider program with the support of legal advice and other relevant expertise and ensure it is fit for purpose across the organisation.

Services Australia response: *Agreed.*

3.19 *Services Australia maintains a mature approach to fraud, corruption and security control assurance and reporting including the management of inside threats as they are detected. The Agency meets and exceeds its fraud control requirements under Section 10 of the Public Governance, Performance and Accountability (PGPA) Rule 2014 and the Commonwealth Fraud Control Framework.*

3.20 *The Agency has currently engaged and is working with the Office of National Intelligence, to improve its insider threat focus. It also works closely with the National Anti-Corruption Commission, Federal and State Law Enforcement, and other Government entities. The Agency is committed to improving its current processes and procedures to better protect against and manage inside threats.*

ANAO comment

3.21 As noted in Table 3.5 and paragraph 3.17, the Australian Signals Directorate's Cyber Security Guideline, *Guidelines for Cyber Security Incidents*, recommends that a trusted insider program is developed, implemented and maintained and that legal advice is sought regarding the development and implementation of a trusted insider program. Services Australia's Integrity Framework was developed, implemented and maintained without advice provided by relevant external entities and internal functions within Services Australia.

3.22 Services Australia has implemented a systems definition and categorisation process, as part of the systems criticality assessment, to gather and assess system information. The process identifies stakeholders including system owners and determines the criticality of the system in relation to security objectives. Each system criticality is endorsed by the system owner as well as the CISO. A number of systems criticality assessments are incomplete and do not define all of Services Australia's critical systems, with a number of critical systems without descriptions, business owners or a systems owners assigned.

Recommendation no. 11

3.23 Services Australia updates its systems criticality assessments and data registers with the necessary information to confirm the criticality of each system and data asset.

Services Australia response: *Agreed.*

3.24 *Services Australia will update and complete the systems criticality register to ensure all critical systems and supporting data sets are included on the register, in support of the assessment of system criticality.*

3.25 Services Australia's Data Asset Management Policy outlines practices for identifying, defining and organising data assets. For each data asset, the data register records information including format; location; security classification; and the data steward. The accuracy of the data

register is reviewed annually by the data steward. Services Australia's Data Asset Management Policy outlines practices for organising data assets, the policy does not specify the criticality of data assets.

3.26 The majority of Services Australia's security documentation was last updated between June 2022 and December 2023. Services Australia does not have documented plans to review, update and test its security documentation.

Cyber security incident management

3.27 Services Australia's documented framework of procedures for cyber security incident management includes its Cyber Security Incident Response Plan and security incident register.

3.28 Services Australia removed 'cyber security incidents' from the Incident Management and Escalation Policy in June 2023, and advised the ANAO in January 2024 that cyber security incidents are managed by the 'relevant business teams' within the Cyber Security Division. Services Australia does not have a policy or approach for managing cyber security incidents. In January 2024, Services Australia advised the ANAO that it would commence the development of its Cyber Security Incident Management and Response Policy in March 2024.

Recommendation no. 12

3.29 Services Australia establishes a Cyber Security Incident Management Policy or include 'cyber security incidents' as part of the scope of the Incident Management and Escalation Policy.

Services Australia response: *Agreed.*

3.30 *Services Australia will establish and implement a Cyber Security Incident Management Policy.*

3.31 A documented approach for triaging and responding is outlined within the Cyber Security Incident Response Plan. There is no monitored email address as the central conduit documented and Services Australia has also not documented:

- a summary of common cyber incident types and initial response activities;
- references to or utilisation of relevant external standards and frameworks; and
- guidance for sector and jurisdictional reporting arrangements.

3.32 Supporting this framework of procedures, Services Australia has documented guidance in the form of playbooks⁸³ which address several adversary tactics.

Security maturity monitoring plan

3.33 Services Australia has a security maturity monitoring plan called the Protective Security Risk Management Plan. The Protective Security Risk Management Plan includes details on:

- developing controls through policies and procedures used to manage incidents and escalations;
- identifying risks and controls to mitigate these risks from being realised; and

⁸³ Document with instructions for managing specific types of cyber security incidents.

- a matrix which identifies which responsible area manages which PSPF policy.

3.34 The Protective Security Risk Management Plan does not detail an approach that defines a continuous improvement cycle as well as reporting to management. The plan does not specify the determination of reporting frequency of security monitoring advice and does not include security maturity indicators that trigger report escalation. Services Australia has not assessed whether the frequency of security monitoring advice and approach to monitoring security performance, including report escalation, is fit-for-purpose for its risk environment.

Recommendation no. 13

3.35 Services Australia develops and implements an approach that ensures continuous monitoring and improvement reporting is provided to management, including documenting the determination of reporting frequency and escalation.

Services Australia response: *Agreed.*

3.36 *Services Australia will update the Protective Security Plan to incorporate specific guidance on continuous monitoring and improvement reporting.*

Internal reporting process

3.37 Services Australia's CISO, with the support of national managers within the Cyber Security Division, is informed through secure communication channels about cyber security incidents which have been prioritised between the second and fourth levels.⁸⁴ For more significant or reportable cyber security incidents which have been prioritised at the highest level, the CISO acts as the incident controller.

3.38 In addition, Services Australia has a security governance committee structure, including cyber security governance, which is outlined within the Cyber Security Governance Framework.⁸⁵ The Framework requires the cyber security function to provide quarterly risk reporting, as well as reporting by exception, to the Cyber Resilience Board and the Strategic Cyber Security CISO Board which are chaired by the CISO. Services Australia reports biannually on any emerging risks or changes to its security environment to the Executive Committee and the Security Committee.

External reporting process

3.39 Services Australia has submitted its PSPF security report as well as completed its ASD cyber security survey annually. Services Australia has not defined reporting timeframes for referring significant or reportable cyber security incidents to ASD, affected entities, affected sectors and jurisdictions, and other notifiable authorities as recommended by ASD's *Cyber Incident Response*

84 Services Australia's cyber security incident severity classifications are rated between 1 and 4, with 1 being the highest severity and 4 being the lowest.

85 The Cyber Security Governance Framework outlines the various governance committees in place and their responsibilities for managing cyber security.

Plan. The *Cyber Incident Response Plan* also recommends that external reporting include a process for how the Department of Home Affairs, as the owner of the PSPF, will be notified.⁸⁶

3.40 Services Australia's Cyber Security Governance Framework requires the cyber security function to provide quarterly risk reporting to the Minister for Government Services. Services Australia does not regularly provide risk reporting to the Minister of Home Affairs and the Minister for Cyber Security.

3.41 The role and responsibilities of Services Australia's legal function during external referrals of significant cyber security incidents has not been outlined within the Cyber Security Incident Response Plan.

3.42 Services Australia demonstrated it did not have any significant or reportable cyber security incidents to report to ASD during the audit period, 1 July 2022 to 31 October 2023. However, Services Australia was notified by the National Cyber Security Coordinator in 2023 that it had been indirectly impacted by a large-scale cyber security incident on HWL Ebsworth Lawyers.⁸⁷

Recommendation no. 14

3.43 Services Australia designs and implements procedures detailing:

- (a) the timeframes for reporting to internal and external stakeholders; and
- (b) roles and responsibilities for coordinating responses, including engagement of relevant expertise.

Services Australia response: *Agreed.*

3.44 *Services Australia will articulate timeframes and roles and responsibilities for reporting to stakeholders within Services Australia's Cyber Security Incident Response Plan.*

Has Services Australia effectively implemented cyber security incident management processes for investigating and responding to cyber security incidents?

Services Australia has documented its approach for managing data spills, malicious code infections and intrusions. It has not established processes for reviewing, updating and testing these cyber security incident response procedures.

Services Australia has implemented a SIEM solution and developed a systematic approach to the monitoring and prioritisation of security alerts.

Services Australia has an Event Logging and Monitoring Policy. It has not established processes for extracting, retrieving and analysing archived SIEM data, nor has it defined the timeframe requirements for triage and escalation activities.

Services Australia has not defined an approach for cyber security investigations.

86 Australian Signals Directorate, *Cyber Incident Response Plan Guidance*, ASD, Canberra, July 2022, available from https://www.cyber.gov.au/sites/default/files/2023-03/ACSC%20Cyber%20Incident%20Response%20Plan%20Guidance_A4.pdf [accessed 8 April 2024], p. 19.

87 See paragraph 1.3.

3.45 The *Information Security Manual* notes that ‘establishing a cyber security incident management policy can increase the likelihood of successfully planning for, detecting and responding to malicious activity’.⁸⁸

3.46 PSPF Policy 2 outlines the management structures and responsibilities for how entities can ensure the effective implementation of security practices for investigating and responding to cyber security incidents. The policy requires that assigned security roles, responsibilities and management structures are defined to enable⁸⁹:

- the coordination or reporting on cyber security;
- the supervision of cyber security incident response activities and crisis management;
- the improvement of business resilience and ensure the continued operation of critical business processes; and
- the alignment of cyber security posture with its business objectives and the PSPF.

3.47 ASD’s *Guidelines for Cyber Security Incidents*⁹⁰ and *Guidelines for System Monitoring*⁹¹ specify that cyber security practices are likely to be more effective and achieve security outcomes when they are well documented, embedded into daily operations and supported by senior management. These guidelines recommend:

- the development of cyber security incident response plans that document an approach to data spills, malicious code infections and intrusions;
- the development of event logging policies;
- the implementation of a centralised event logging facility; and
- the establishment of security practices that ensure the integrity of evidence following a cyber security incident.

3.48 As outlined in paragraph 1.29, Services Australia self-assessed as Substantial for PSPF Policy 2 in 2022–23.

3.49 The compliance of Services Australia’s security plans, documentation and evidence of its implementation of PSPF Policy 2 and ASD’s *Guidelines for Cyber Security Incidents* and *Guidelines for System Monitoring* is summarised in Tables 3.7 to 3.9. Of these seven requirements, four were fully implemented, two were partly implemented and one was not implemented.


88 Australian Signals Directorate, ‘Guidelines for Cyber Security Incidents’ webpage, ASD, Canberra, last updated 1 March 2024, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents> [accessed on 8 April 2024].

89 Department of Home Affairs, *Protective Security Policy Framework — 2 Management structures and responsibilities*, Home Affairs, Canberra, 2018 (last updated 30 August 2023), available from <https://www.protectivesecurity.gov.au/system/files/2023-08/policy-02-management-structures-and-responsibilities.pdf> [accessed on 8 April 2024], p. 3.

90 Australian Signals Directorate, ‘Guidelines for Cyber Security Incidents’ webpage, ASD, Canberra, last updated 1 March 2024, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents> [accessed on 8 April 2024].

91 Australian Signals Directorate, ‘Guidelines for System Monitoring’ webpage, ASD, Canberra, last updated 1 December 2023, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-system-monitoring> [accessed on 8 April 2024].

Table 3.7: Services Australia's implementation of PSPF Policy 2 — Management structures and responsibilities


PSPF Policy 2 requirements	ANAO assessment	ANAO comment
<p>Entities must develop and use procedures that ensure:</p> <ul style="list-style-type: none"> all elements of the entity's security plan are achieved; security incidents are investigated, responded to, and reported; and relevant security policy or legislative obligations are met. 		<p>Services Australia has designed and implemented a framework of procedures for responding to cyber security incidents. Services Australia has an Incident Management and Escalation Policy. However, Services Australia removed 'cyber security incidents' from the Incident Management and Escalation Policy in June 2023, and advised the ANAO in January 2024 that cyber security incidents are managed by the 'relevant business teams' within the Cyber Security Division.</p> <p>The majority of Services Australia's security documentation was last updated between June 2022 and December 2023. Services Australia does not have a documented plan to review, update and test its security documentation.</p> <p>Services Australia's CISO, with the support of national managers within the Cyber Security Division, is informed, through secure communication channels, about cyber security incidents which have been prioritised between the second and fourth levels.^a For more significant or reportable cyber security incidents which have been prioritised at the highest level, the CISO acts as the incident controller.</p>




Key:  Fully implemented  Partly implemented  Not implemented

Note a: Services Australia's cyber security incident severity classifications are rated between 1 and 4, with 1 being the highest severity and 4 being the lowest.

Source: ANAO analysis of Services Australia's implementation of *PSPF Policy 2 — Management structures and responsibilities*.

Table 3.8: Services Australia's implementation of ASD's Guidelines for Cyber Security Incidents



Guideline recommendations	ANAO assessment	ANAO comment
<p>When a data spill occurs, data owners are advised and access to the data is restricted.</p>		<p>Services Australia has designed and implemented procedures for handling data spills. However, it has not detailed an approach for containing data spills. A plan of containment is determined on a case-by-case basis based on operational team discussions.</p> <p>Services Australia has not developed an inventory of important datasets and their associated owners.</p>

Guideline recommendations	ANAO assessment	ANAO comment
<p>When malicious code is detected, the following steps are taken to handle and contain malicious code infections:</p> <ul style="list-style-type: none"> a) the infected systems are isolated b) all previously connected media used in the period leading up to the infection are scanned for signs of infection and isolated if necessary c) antivirus software is used to remove the infection from infected systems and media; and d) if the infection cannot be reliably removed, systems are restored from a known good backup or rebuilt. 		<p>Services Australia does documented approach for containing malicious code infections that details the recommended steps.</p>
<p>When an intrusion is detected, the following steps are taken to handle and contain the intrusion:</p> <ul style="list-style-type: none"> a) Legal advice is sought before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence. b) System owners are consulted before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence. c) Planning and coordination of intrusion remediation activities are conducted on a separate system to that which has been compromised. d) To the extent possible, all intrusion remediation activities are conducted in a coordinated manner during the same planned outage. e) Following intrusion remediation activities, full network traffic is captured for at least seven days and analysed to determine whether the adversary has been successfully removed from the system. 		<p>Services Australia does have a documented approach for handling and containing intrusions that details the recommended steps.</p>
<p>The integrity of evidence gathered during an investigation is maintained by investigators in the following way:</p> <ul style="list-style-type: none"> a) recording all of their actions b) maintaining a proper chain of custody; and c) following all instructions provided by relevant law enforcement agencies. 		<p>Services Australia has not documented its approach to cyber security investigations of compromised servers, end-user computers and mobile phones or referred to the Australian Government Investigations Standard as the guidance to be used by its investigators.</p>

Key:  Fully implemented  Partly implemented  Not implemented

Source: ANAO analysis of Services Australia's implementation of ASD's *Guidelines for Cyber Security Incidents*.

Table 3.9: Services Australia's implementation of ASD's *Guidelines for System Monitoring*

Guideline recommendations	ANAO assessment	ANAO comment
<p>A centralised event logging facility is implemented in the following way:</p> <ul style="list-style-type: none"> a) event logs are sent to the facility as soon as possible after they occur; b) event logs are protected from unauthorised modification and deletion; and c) an accurate time source is established and used consistently across systems to assist with identifying connections between events. 		<p>Services Australia has implemented a centralised event logging facility approach in the recommended way.</p>
<p>Cyber security events are analysed in a timely manner to identify cyber security incidents.</p>		<p>Services Australia has implemented a process for identifying, investigating, triaging and escalating cyber security incidents.</p> <p>Services Australia has not designed and implemented a policy for how to analyse cyber security events in a timely manner.</p>

Key:  Fully implemented  Partly implemented  Not implemented

Source: ANAO analysis of Services Australia's implementation of ASD's *Guidelines for System Monitoring*.

Cyber security incident response procedures

3.50 As outlined at paragraph 3.27, Services Australia's has a documented framework of procedures for cyber security incident management. This framework includes procedures for responding to cyber security incidents.

3.51 Services Australia has documented associated guidance for cyber security incident response which includes:

- Privacy Incident and Data Breach Response Plan;
- Data Asset Management Policy;
- Cyber Security Incident Response Plan;
- Event Logging and Monitoring Policy;
- systems criticality assessment; and
- playbooks which address several adversary tactics.

Management of data spills and malicious code

3.52 Services Australia's Privacy Incident and Data Breach Response Plan documents the approach to managing data spills. Data spills are managed by the Privacy and Personal Information Release Branch with the support of the Cyber Operations Branch.

3.53 The Privacy Incident and Data Breach Response Plan requires staff to report an ‘eligible data breach’ to the Privacy and Personal Information Release Branch immediately so that the Privacy and Personal Information Release Branch can:

- undertake an assessment within 30 days;
- contain and remediate the data breach as soon as possible; and
- notify the Office of the Australian Information Commissioner (OAIC) and affected stakeholders as soon as practicable.

3.54 Services Australia’s processes require the restriction of access to data, systems and networks in the event of a data spill. In addition, they cover the handling and containing of malicious code infections; and intrusions.

Management of remediation activities

3.55 Services Australia’s Cyber Security Incident Response Plan outlines roles and responsibilities across the cyber security incident management process, with the CISO as the Incident Controller.⁹²

3.56 The Incident Coordinator has responsibility to assess and determine whether the cyber security incident is a priority across Services Australia and its shared service entities. This includes incidents within Services Australia and for its shared service entities with respect to IT and cyber security services.⁹³ The Incident Controller is responsible for assigning the severity ratings of security incidents. The Incident Controller is supported by the Cyber Security Incident Response Team (CSIRT). The CSIRT is responsible for managing remediation activities, including the performance of investigations, analysis and evaluations.

3.57 Where there are incidents and events outlined in the Cyber Security Incident Response Plan which require further investigation or if the incident or event is a privacy incident or a data breach, the Legal Services Division acts as the Designated Privacy Officer within Services Australia. The Incident Controller is responsible for communicating the incident response within Services Australia and to shared service entities.

3.58 Services Australia has not documented its approach to cyber security investigations. Although cyber security investigations are performed by the CSIRT, there are no documented procedures that ensure cyber security investigations are performed in accordance with the Australian Government Investigations Standard. Services Australia has not defined:

- when communications relating to cyber security incidents are moved to, or recorded in, its archive systems after a cyber security incident has been finalised; and
- how the principles of maintaining the integrity of evidence would be observed during a cyber security investigation.

92 Services Australia’s Incident Controller is responsible for the management and coordination of the Cyber Security Incident Response Team and other relevant supporting operational teams.

93 The shared service entities for IT security services are the National Disability Insurance Agency, Department of Veterans’ Affairs and the Department of Social Services.

Recommendation no. 15

3.59 Services Australia develops and implements procedures detailing:

- (a) the process for performing cyber security investigations in accordance with the Australian Government Investigations Standard; and
- (b) the process for managing and maintaining evidence during and after cyber security investigations.

Services Australia response: *Agreed.*

3.60 *Services Australia has a mature investigative capability to support the Agency response when incidents occur or are referred to the appropriate lead agency, in particular the Australian Federal Police (AFP). The Agency has documented processes for the gathering, managing and maintaining of evidence during investigations, in a manner that is consistent with the Australian Government Investigation Standards (AGIS).*

3.61 *The Agency acknowledges there are opportunities to better document processes for investigating cyber security incidents, particularly in relation to roles and responsibilities, accountabilities and hand-off points as between key stakeholders within the Agency. This includes processes to ensure the effective capture and preservation of evidence during the course of investigations of cyber security incidents.*

3.62 Services Australia uses alternative communications channels to plan and coordinate remediation and investigation activities, as well as using a physical 'war room'.⁹⁴ The use of a separate system enables Services Australia to continue with remediation activities outside of the compromised system.

3.63 Services Australia has the ability to capture network traffic for the purposes of remediation and investigation activities.

3.64 As outlined at paragraph 3.42, the CISO was involved in resolving the notification from the National Cyber Security Coordinator as the Incident Controller, and was supported by general counsel and the general manager of fraud control. This matter was finalised in accordance with guidance from Services Australia's Third-party Compromise Plan within three months.

Security Information and Event Management solution

3.65 Services Australia has had a Security Information and Event Management (SIEM) solution in place since 2018 and employs a centralised logging model with respect to its management. Services Australia prioritises its event monitoring resources using an appropriate framework. Services Australia has not implemented ASD's recommendation for appropriate SIEM coverage. It uses an alternative cyber security framework to provide SIEM coverage. Services Australia uses a heat map of security alerts to monitor several platforms across its IT environment. This heat map covers Services Australia's major platforms.

⁹⁴ A war room is a place where responders and stakeholders can gather to work through a major incident. When a major incident occurs, many teams prefer to gather all subject matter experts to resolve the problem as quickly as possible.

3.66 Services Australia’s Event Logging and Monitoring Policy outlines the approach for managing security event logs. The CISO and system owners have implemented mechanisms to enable the processing of event log data from business systems to the SIEM solution. Event log processing is reviewed daily by SIEM administrators. Any processing failures are remediated using the SIEM solution in accordance with Services Australia’s SIEM standard operating procedures.

3.67 The SIEM solution contains configured security alerts that trigger when configured conditions or rules are fulfilled during event log processing.⁹⁵ The security alert configuration is reviewed daily by SIEM administrators to ensure current security threats are detected. Services Australia has established a team that updates its playbooks following incident management, although every time staff use a playbook they are meant to reflect on how the playbook can be improved and update the playbook if required.

3.68 Services Australia’s Event Logging and Monitoring Policy was issued in June 2016 and last updated in June 2021. Services Australia does not have documented plans to review, update and test the policy.

Analysis of cyber security events

3.69 Services Australia’s process for prioritising and triaging security alerts is largely automated with limited human intervention. The SIEM solution assigns the ‘offense’ to a security alert.⁹⁶ The security alert is investigated by security analysts, who then initiate the required remediation actions. Evidence, working notes and conclusions as well as security analyst details are recorded directly against each offense in the SIEM solution. Unassigned offenses appear on the SIEM solution’s dashboard and are monitored by the security analysts, until they can be prioritised and triaged as needed.

3.70 Services Australia has not defined timeframes for analysing cyber security events, nor does it perform any analysis on the timeliness of triaging and escalation processes. When requested by the ANAO, Services Australia could not provide all archived offense data from 1 June 2022 to 31 October 2023. Services Australia does not have a process for extracting, retrieving and analysing cyber security events from archives for future analysis. Services Australia analyses non-archived SIEM solution data, specifically offense data, on a daily basis.

Recommendation no. 16

3.71 Services Australia develops and implements:

- (a) a process for retrieving and analysing archived Security Information and Event Management (SIEM) solution data; and
- (b) timeframe requirements for triage and escalation activities.

Services Australia response: *Agreed.*

95 Services Australia refers to triggered conditions or rules as an ‘offense’. See paragraph 3.69.

96 The SIEM solution will assign ‘offense’ to a customised security alert based on a series of ratings in addition to providing a summary as well as an overall magnitude rating taking into account system criticality among other considerations.

3.72 *Services Australia will develop and implement a procedure for more timely restoration of archived SIEM data and the analysis of this data. Additionally, Services Australia will also develop timeframes required for triage and escalation activities.*

3.73 The ANAO analysed the timeliness of a cyber security response using a sample of offense data for the period of 20 July 2023 to 30 August 2023. Ninety-five per cent of offenses were triaged⁹⁷ within 12 hours and then investigated within 11 hours. High priority offenses were triaged within an hour and investigated within 13 hours.

Has Services Australia effectively implemented recovery processes that mitigate disruptions during and after cyber security incidents?

Services Australia has not defined an approach to digital preservation related to cyber security incidents and regular backups nor does it have business continuity or disaster recovery plans that address all systems, including the systems which support the critical recovery processes. It is not well placed to ensure business continuity or disaster recovery in the event of a significant or reportable cyber security incident.

Services Australia has processes for performing regular backups. These processes do not include all platforms and Services Australia does not test the restoration of data, applications and settings from backups to a common point in time as part of disaster recovery exercises.

Services Australia has not appropriately documented an embedded post-incident learning approach following a cyber security incident.

Services Australia has not established a process that leverages post-incident learnings to review and improve the effective implementation of arrangements to manage cyber security incidents.

3.74 The *Information Security Manual* notes that 'establishing a cyber security incident management policy can increase the likelihood of successfully planning for, detecting and responding to malicious activity'.⁹⁸ Such arrangements could mitigate disruption to business operations during and after cyber security incidents and enable entities to recover data as well as the systems, applications and servers supporting critical business processes.⁹⁹

3.75 The PSPF Policy 10 requires entities to implement regular backup processes.¹⁰⁰ PSPF Policy 2 outlines the required management structures and responsibilities for implementing Policy 10

97 Number of hours for assessing the priority and severity of offense.

98 Australian Signals Directorate, 'Guidelines for Cyber Security Incidents' webpage, ASD, Canberra, last updated 1 March 2024, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents> [accessed on 8 April 2024].

99 *ibid.*

100 Department of Home Affairs, *Protective Security Policy Framework — 10 Safeguarding data from cyber threats*, Home Affairs, Canberra, 2018 (last updated 18 February 2024), available from <https://www.protectivesecurity.gov.au/system/files/2024-02/policy-10-safeguarding-data-from-cyber-threats.pdf> [accessed on 8 April 2024], p. 2 (item B.1.a.viii).

requirements, coordinating cyber security incident recovery activities as well as implementing post-incident learning to improve cyber security incident management arrangements.¹⁰¹

3.76 ASD's *Guidelines for Cyber Security Roles*¹⁰², *Guidelines for Cyber Security Incidents*¹⁰³ and the *Essential Eight Maturity Model*¹⁰⁴ specify how entities can effectively implement arrangements for cyber security incident response processes. These guidelines:

- highlight the importance of the CISO role for overseeing cyber security incident response activities and contributing to business continuity and disaster recovering planning;
- recommend how entities enact their cyber security incident response plans following the identification of a cyber security incident; and
- recommend how entities can implement the Essential Eight mitigation strategies.

3.77 The Essential Eight mitigation strategies are the most effective of 37 prioritised mitigation strategies outlined in ASD's *Strategies to Mitigate Cyber Security Incidents*.¹⁰⁵ The essential mitigation strategy for recovering data and system availability is called 'Regular backups'.

3.78 As outlined in paragraph 1.29, Services Australia self-assessed as Substantial for PSPF Policy 2 and Partial for PSPF Policy 10 across the financial year 2022–23.

3.79 The compliance of Services Australia's cyber security incident recovery documentation as well as evidence of its implementation of PSPF Policies 2 and 10 as well as ASD's *Guidelines for Cyber Security Roles*, *Guidelines for Cyber Security Incidents* and the *Essential Eight Maturity Model* are summarised in Tables 3.10 to 3.14. Of the nine requirements, four were implemented, three were partly implemented, and two were not implemented.

101 Department of Home Affairs, *Protective Security Policy Framework — 2 Management structures and responsibilities*, Home Affairs, Canberra, 2018 (last updated 30 August 2023), available from <https://www.protectivesecurity.gov.au/system/files/2023-08/policy-02-management-structures-and-responsibilities.pdf> [accessed on 8 April 2024], p. 3.




102 Australian Signals Directorate, 'Guidelines for Cyber Security Roles' webpage, ASD, Canberra, last updated 1 March 2024, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-roles> [accessed on 8 April 2024].

103 Australian Signals Directorate, 'Guidelines for Cyber Security Incidents' webpage, ASD, Canberra, last updated 1 March 2024, available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/ism/cyber-security-guidelines/guidelines-cyber-security-incidents> [accessed on 8 April 2024], pp. 11–15.

104 Australian Signals Directorate, 'Essential Eight Maturity Model' webpage, ASD, Canberra, June 2017 (last updated November 2023) available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model> [accessed 8 April 2024].

105 Australian Signals Directorate, 'Strategies to Mitigate Cyber Security Incidents' webpage, ASD, Canberra, February 2010 (last updated February 2017), available from <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents/strategies-mitigate-cyber-security-incidents> [accessed 8 April 2024].

Table 3.10: Services Australia's implementation of PSPF Policy 2 — Management structures and responsibilities

PSPF Policy 2 requirements	ANAO assessment	ANAO comment
<p>Entities must develop and use procedures that ensure:</p> <ul style="list-style-type: none"> all elements of the entity's security plan are achieved; security incidents are investigated, responded to, and reported; and relevant security policy or legislative obligations are met. 		<p>Services Australia has designed and implemented a framework of procedures for recovering from cyber security incidents.</p> <p>Services Australia has an Incident Management and Escalation Policy. However, Services Australia removed 'cyber security incidents' from the Incident Management and Escalation Policy in June 2023, and advised the ANAO that cyber security incidents are managed by the 'relevant business teams' within the Cyber Security Division.</p> <p>The majority of Services Australia's security documentation was last updated between June 2022 and December 2023. Services Australia does not have a documented plan to review, update and test its security documentation.</p> <p>Services Australia's CISO, with the support of national managers within the Cyber Security Division, is informed, through secure communication channels, about cyber security incidents which have been prioritised between the second and fourth levels. For more significant or reportable cyber security incidents which have been prioritised at the highest level, the CISO acts as the incident controller.</p>
<p>A process of continual improvement be applied to monitoring, evaluating, responding to and managing security incidents.</p>		<p>Services Australia has a security maturity monitoring plan called the Protective Security Risk Management Plan, although it has not defined a continuous improvement cycle as well as reporting to management.</p>
<p>Entities identify, document and share learnings internally ... and externally, where appropriate.</p>		<p>Services Australia does not use incident reports to update its framework of procedures for cyber security incident management or share learnings internally and externally, where appropriate.</p>

Key:  Fully implemented  Partly implemented  Not implemented

Source: ANAO analysis of Services Australia's implementation of PSPF Policy 2 — Management structures and responsibilities.

Table 3.11: Services Australia’s implementation of PSPF Policy 10 — Safeguarding data from cyber threats

PSPF Policy 10 requirements	ANAO assessment	ANAO comment
Each entity must mitigate common cyber threats by implementing the following mitigation strategies from the <i>Strategies to Mitigate Cyber Security Incidents</i> : ... regular backups	▲	Services Australia has a regular backup solution in place. However, the approach is not supported by an appropriately designed and implemented policy.

Key: ◆ Fully implemented ▲ Partly implemented ■ Not implemented.

Source: ANAO analysis of Services Australia’s implementation of PSPF Policy 10 — Safeguarding data from cyber threats.

Table 3.12: Services Australia’s implementation of ASD’s Guidelines for Cyber Security Roles

Guideline recommendations	ANAO assessment	ANAO comment
The CISO contributes to the development and maintenance of business continuity and disaster recovery plans for their organisation to ensure that business-critical services are supported appropriately in the event of a disaster.	◆	Services Australia has designed and implemented assigned responsibilities for its CISO; such as, contributing to the development and maintenance of business continuity and disaster recovery plans.

Key: ◆ Fully implemented ▲ Partly implemented ■ Not implemented

Source: ANAO analysis of Services Australia’s implementation of ASD’s Guidelines for Cyber Security Roles.

Table 3.13: Services Australia’s implementation of ASD’s Guidelines for Cyber Security Incidents

Guideline recommendations	ANAO assessment	ANAO comment
Following the identification of a cyber security incident, an organisation’s incident response plan and business continuity is enacted.	◆	Services Australia’s Business Continuity Plan and Cyber Security Incident Response Plan are enacted by the CISO during the relevant incident or business continuity event.

Key: ◆ Fully implemented ▲ Partly implemented ■ Not implemented

Source: ANAO analysis of Services Australia’s implementation of ASD’s Guidelines for Cyber Security Incidents.

Table 3.14: Services Australia's implementation of ASD's *Essential Eight Maturity Model*

Guidance recommendation	ANAO assessment	ANAO comment
Backups of important data, software and configuration settings are implemented in the recommended way: a) performed and retained with a frequency and retention timeframe in accordance with business continuity requirements b) synchronised to enable restoration to a common point in time; and c) retained in a secure and resilient manner.	▲	Services Australia has a regular backup solution in place which is largely implemented in the recommended way. However, has not enabled restoration of backups to a common point in time once it has been archived.
Unprivileged and privileged accounts (excluding backup administrator accounts): a) cannot access backups belonging to other accounts; and b) are prevented from modifying and deleting backups.	◆	Services Australia has implemented security controls to ensure that regular backups are stored in a secure and resilient manner and access, modification and deletion of backups is restricted appropriately.
Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.	■	Services Australia's recovery processes are not tested as part of disaster recovery exercises.

Key: ◆ Fully implemented ▲ Partly implemented ■ Not implemented

Source: ANAO analysis of Services Australia's implementation of ASD's *Essential Eight Maturity Model*.

Cyber security incident recovery procedures

3.80 As outlined at paragraph 3.27, Services Australia has a documented framework of procedures for cyber security incident management. This framework includes procedures for recovering from cyber security incidents.

3.81 Services Australia has also documented associated guidance for cyber security incident recovery which includes:

- Cyber Security Incident Response Plan;
- Business Continuity Plan;
- Disaster Recovery Testing Schedule;
- Privacy Incident and Data Breach Response Plan; and
- systems criticality assessment.

3.82 Services Australia has not defined an approach to digital preservation. The concept of 'digital preservation' is mentioned within the Records Management Policy. This relates to appropriate protective marking and ensuring compliance with the *Archives Act 1983* when creating, managing and disposing of records. The policy does not consider the long-term availability and integrity of

Services Australia's data, as well as the degradation and removable media, hardware and software obsolescence.

3.83 The Cyber Security Incident Response Plan and the Business Continuity Plan are high-level governance documents outlining the response processes, communication, and continuity planning requirements. The cyber security incident recovery process is outlined in the Business Continuity Plan.¹⁰⁶ The Cyber Security Incident Response Plan is required to be enacted early in the detection phase, where events are prioritised by severity ratings and are managed by the CISO. The Business Continuity Plan is required to be enacted as soon as business functions are disrupted. These plans can be enacted by the National Manager of Cyber Capabilities, the Response and Recovery Committee, or the ICT Response and Recovery Committee.

3.84 The Business Continuity Plan outlines the recovery time objectives and maximum tolerable periods of disruption for a list of business processes. Services Australia does not have business continuity or disaster recovery plans that address all systems, including the systems which support the critical recovery processes. Services Australia does not have a complete list of critical assets. As such, Services Australia is not well placed to ensure business continuity or disaster recovery in the event of a significant or reportable cyber security incident.

3.85 Services Australia has a Disaster Recovery Testing Schedule dated 31 October 2023. This schedule did not include all the systems within Services Australia. This schedule was later updated by Services Australia to include three significant financial systems, Medicare, Payment Assessment Calculation Engine (PACE) and Child Support IT system (Cuba).¹⁰⁷ This schedule update was the result of issues identified during the audit of Services Australia's 2023–24 financial statements.

While additional systems were included in this update, the approach to testing was not detailed and the business and system owners and criticality of the systems were not defined.

3.86 Services Australia does not have a policy for managing regular backups. Services Australia's recovery documentation does not include:

- regular backup solutions within its security policies;
- regular backup solutions in its disaster recovery testing schedule;
- the approach to prioritising encryption of regular backups; and
- details of protection measures for backup media devices.

106 Services Australia's cyber security incident recovery process is a three-step process covering incident response; business continuity; and resumption.

107 The Medicare system supports Australia's national health insurance scheme, Medicare, and assists with processing payments for hospital, medicine and medical services. PACE is the system used to support Residential Aged Care processes. Cuba is the system that supports Child Support processes.

Recommendation no. 17

3.87 Services Australia develop and implement:

- (a) A policy for digital preservation;
- (b) a policy for regular backups;
- (c) business continuity and disaster recovery plans that include the systems, applications and servers which support their critical recovery processes; and
- (d) processes that test the recoverability of their systems and applications supporting critical business processes, and implement any lessons learned into future testing plans.

Services Australia response: *Agreed.*

3.88 Services Australia will develop and implement policies for digital preservation, data backup and restoration. These policies will form part of the Agency's revised approach to disaster recovery and business continuity planning which will define critical business processes, systems and services and plan the testing for recoverability of systems and servers with lessons learnt being incorporated into future disaster recovery testing.

3.89 Services Australia has a Privacy Incident and Data Breach Response Plan which outlines the management of privacy incidents or data breaches; notifiable data breaches reporting timeframes; roles and responsibilities; and post-incident reviews.

Performing and retaining regular backups

3.90 As outlined in Table 3.11, a policy for regular backups has not been designed and implemented. Services Australia has processes for performing regular backups. However, not all platforms are included. Regular backups are retained for a maximum period of 42 days, with standardised schedules and retention periods specified for databases and operating systems.

3.91 The backup requirements are defined by the relevant systems subject matter expert. These requirements are provided to the backup administration team that configures Services Australia's backup solutions accordingly. The backup administration team review the processing of backups daily to ensure backups are successfully completed.

3.92 There are three data centres across two sites that serve as Services Australia's primary data centres and have been assessed by the Digital Transformation Agency as providing the highest level of security assurance under the Hosting Certification Framework. There is an additional data centre which serves as a disaster recovery site for Services Australia's primary data centres.

Restricting access to backups

3.93 Services Australia has security controls to ensure that regular backups are stored in a secure and resilient manner. Services Australia uses retention locks to control access to backup data. These locks prevent the modification, deletion and removal of backup data for a specified retention period.

Regular testing of backups

3.94 Services Australia does not test the restoration of data, applications and settings from backups to a common point in time as part of disaster recovery exercises.

3.95 A desktop exercise was conducted in June 2022 and the next one is scheduled to be conducted in April 2024. The lack of evidence of regular testing of backups makes it difficult for Services Australia to assure that it can restore important data and software settings after a disaster recovery event to enable it to continue operating its business.

Recommendation no. 18

3.96 Services Australia establish a program that assesses the effectiveness of recovery processes for all production and archived backup data.

Services Australia response: *Agreed.*

3.97 *Services Australia will implement a process to measure and improve the effectiveness of recovery processes for the Agency's production and archived backup data, applicable to all platforms.*

Appropriately documented and embedded post-incident learning approach

3.98 As outlined at Table 3.5, the Incident Management and Escalation Policy does not include 'cyber security incidents'. Services Australia does not:

- undertake post-incident reviews specific to cyber security events such as cyber security incidents; and
- identify, document or share learnings specific to cyber security incidents.

3.99 In January 2024, Services Australia advised the ANAO that it would commence developing the Cyber Security Incident Management and Response Policy from March 2024.

3.100 As outlined in paragraph 3.42, Services Australia was notified of a cyber security incident that may impact its business. Any lessons learned from that experience, including support received from Services Australia's legal function, have not been used to review or update Services Australia's framework of procedures for cyber security incident management. Services Australia has not undertaken a post-incident review or a lessons-learned exercise following a large-scale data breach involving HWL Ebsworth Lawyers.

Recommendation no. 19

3.101 Services Australia develops its post-incident learning approaches following a cyber security incident to inform a process that reviews, updates and tests all of the relevant security documentation for the effective management of cyber security incidents. That is:

- (a) supporting security documentation to their security plans;
- (b) framework of procedures for cyber security incident management;
- (c) associated guidance for cyber security incident response; and
- (d) associated guidance for cyber security incident recovery.

Services Australia response: *Agreed.*

3.102 *Services Australia will document and embed a post-incident learning approach to ensure that key security documentation and procedures are reviewed for efficacy following a cyber security incident, with updates applied where necessary.*

3.103 *This revised approach will ensure that Services Australia is leveraging learnings following a cyber security incident to improve the ongoing effectiveness of the Agency's cyber incident management process.*



Rona Mellor PSM
Acting Auditor-General

Canberra ACT
14 June 2024

Appendices

Appendix 1 Entity responses

Australian Transaction Reports and Analysis Centre response



Australian Government
AUSTRAC

Chief Executive Officer

23 May 2024

Ms Rona Mellor PSM
Acting Auditor General
Australian National Audit Office

By email: OfficeoftheAuditorGeneralPerformanceAudit@anao.gov.au

Dear Ms Mellor

AUSTRAC Response to the ANAO Proposed Report under s.19 of the Auditor-General Act 1997 Management of Cyber Security Incidents

AUSTRAC welcomes the opportunity from the Australian National Audit Office (ANAO) to provide a response to the summary and recommendations detailed in 'Proposed Report under s.19 of the Auditor-General Act 1997, Management of Cyber Security Incidents - Australian Transaction Reports and Analysis Centre' (the Proposed Report).

AUSTRAC notes that the ANAO made recommendations in 9 key areas for improvement to AUSTRAC's processes and policies for management of cyber security incidents. AUSTRAC accepts all the ANAO recommendations.


AUSTRAC maintains our self-assessment that we are able to respond to cyber security incidents as they occur. AUSTRAC has delivered on our applied practice approach to effective management of cyber security incidents including prioritisation, record keeping, escalation, and seeking internal and external expertise to inform AUSTRAC's effective cyber security incident response. AUSTRAC notes the ANAO's recommendations, which will support AUSTRAC to strengthen our approach to cybersecurity incident management through greater clarity and certainty provided by documenting much of our existing approach and enhancing it where gaps have been identified.

AUSTRAC acknowledges the ANAO's efforts to ensure the Proposed Report does not include overly sensitive security information. AUSTRAC has identified one further reference, the disclosure of which may unnecessarily increase AUSTRAC's security exposure⁶. This reference is included in the attached detailed response document.

The following table addresses each recommendation with AUSTRAC's initial plans for remediation. Further detail on certain matters of expression in the report are addressed in the detailed attachment.

Correspondence: PO Box K534 Haymarket NSW 1240 P: 02 9950 0055 www.austrac.gov.au

Fighting financial crime, together



AUSTRAC thanks the ANAO for your ongoing collaboration throughout this audit.

Yours sincerely



Brendan Thomas
Chief Executive Officer

Correspondence: PO Box K534 Haymarket NSW 1240

P: 02 9950 0055

www.austrac.gov.au



Fighting financial crime, together

ANAO comment on Australian Transaction Reports and Analysis Centre's response

- (a) As discussed in paragraph 9 and 10, the interests of accountability and transparency must be balanced with the need to manage cyber security risks. To assist in appropriately balancing the interests of accountability and potential risk exposure through transparent audit reporting, the ANAO engaged with the Australian Signals Directorate (ASD) to better understand the evolving nature and extent of risk exposure that may arise through the disclosure of technical information in the audit report. This report therefore focuses on matters material to the audit findings against the objective and criteria and contains less detailed technical information than previous audits.

Services Australia response



Australian Government
Services Australia

Our Ref: EC24-001766

Chief Executive Officer
David Hazlehurst

Ms Rona Mellor PSM
Acting Auditor-General
Australian National Audit Office
GPO Box 707
CANBERRA ACT 2601

Dear Ms Mellor 

Service Australia's response to the Australian National Audit Office's (ANAO) performance audit of *Management of Cyber Security Incidents*.

Thank you for providing Services Australia (the Agency) with the opportunity to comment on the ANAO's performance audit, *Management of Cyber Security Incidents*.

I note the audit's overall conclusion that the implementation of arrangements by my Agency to manage cyber security incidents has been partly effective, as well as the opportunities to strengthen our incident management and investigation procedures, and processes for ensuring business continuity or disaster recovery in the event of a significant or reportable cyber security incident.

The Agency takes its responsibility to safeguard the personal information and data of its customers very seriously, as well as the need to ensure continuity of the essential services and payments that the Agency provides. I appreciate the recommendations made in the report are directed towards strengthening the Agency's ability to deliver these outcomes, and we recognise the identified opportunities to improve our processes and procedures to better achieve these objectives.

I would like to thank the ANAO for its cooperative and professional approach throughout the audit process.

Yours sincerely



David Hazlehurst

14 May 2024

Appendix 2 Improvements observed by the ANAO

1. The existence of independent external audit, and the accompanying potential for scrutiny improves performance. Improvements in administrative and management practices usually occur: in anticipation of ANAO audit activity; during an audit engagement; as interim findings are made; and/or after the audit has been completed and formal findings are communicated.

2. The Joint Committee of Public Accounts and Audit (JCPAA) has encouraged the ANAO to consider ways in which the ANAO could capture and describe some of these impacts. The ANAO's Corporate Plan states that the ANAO's annual performance statements will provide a narrative that will consider, amongst other matters, analysis of key improvements made by entities during a performance audit process based on information included in tabled performance audit reports.

3. Performance audits involve close engagement between the ANAO and the audited entity as well as other stakeholders involved in the program or activity being audited. Throughout the audit engagement, the ANAO outlines to the entity the preliminary audit findings, conclusions and potential audit recommendations. This ensures that final recommendations are appropriately targeted and encourages entities to take early remedial action on any identified matters during the course of an audit. Remedial actions entities may take during the audit include:

- strengthening governance arrangements;
- introducing or revising policies, strategies, guidelines or administrative processes; and
- initiating reviews or investigations.

4. In this context, the below actions were observed by the ANAO during the course of the audit. It is not clear whether these actions and/or the timing of these actions were planned in response to proposed or actual audit activity. The ANAO has not sought to obtain assurance over the source of these actions or whether they have been fully implemented.

Australian Transaction Reports and Analysis Centre

- AUSTRAC has undertaken a project to establish a data inventory outlining important datasets and associated owners with an expected completion date of November 2024.

Services Australia

- Services Australia last updated the Privacy Incident and Data Breach Response Plan in November 2023, noting that a desktop exercise on the Digital Identity Exchange was conducted in May 2023 to address a recommendation from an assessment by the Office of the Australian Information Commissioner. In addition, the Privacy Incident and Data Breach Response Plan, Business Continuity Plan, and Protective Security Risk Management Plan were updated during the audit.
- Services Australia updated its Disaster Recovery Testing Schedule on 31 October 2023.

Appendix 3 PSPF Policies 2, 4, 5 and 10 — requirements

Box 1: Protective Security Policy Framework, Policy 2 requirements

Core requirement

The accountable authority must:

- a. appoint a Chief Security Officer (CSO) at the Senior Executive Service level with a minimum security clearance of Negative Vetting Level 1, to be responsible for protective security in the entity
- b. empower the CSO to make decisions about:
...
 - iv. investigating, responding to, and reporting on security incidents (other than cyber incidents).
...
- c. appoint a Chief Information Security Officer (CISO) with appropriate capability and experience and a minimum security clearance of Negative Vetting Level 1, to be responsible for cyber security in the entity
- d. empower the CISO to make decisions about:
...
 - v. investigating, responding to, and reporting on cyber incidents.
...

Supporting requirement 1. Security advisors

- a. The CSO must be responsible for directing all areas of security to protect the entity's people, information and assets. This includes appointing security advisors to support them in the day-to-day delivery of protective security and, to perform specialist services.
- b. The CISO must be responsible for the entity's cyber security program and associated implementation program. This includes appointing cyber security advisors to support them in the day-to-day delivery of cyber security, and to perform specialist services.

Supporting requirement 2. Security procedures

Entities must develop and use procedures that ensure:

- a. all elements of the entity's security plan are achieved
- b. security incidents are investigated, responded to, and reported
- c. relevant security policy or legislative obligations are met.

...

Supporting requirement 5. General email

Entities must maintain a monitored email address as the central conduit for all security-related matters across governance, personnel, information, cyber and physical security.

Box 2: Protective Security Policy Framework, Policy 4 requirements**Core requirement**

Each entity must assess the maturity of its security capability and risk culture by considering its progress against the goals and strategic objectives identified in its security plan.

Supporting requirement 1. Security maturity records

Entities must document and evidence their assessment of [their] security [capability] maturity.

Box 3: Protective Security Policy Framework, Policy 5 requirements**Core requirement**

Each entity must report on security:

- a. each financial year to its Portfolio Minister and the Department of Home Affairs ...
- b. to affected entities whose interests or security arrangements could be affected by the outcome of unmitigated security risks, security incidents or vulnerabilities in PSPF implementation
- c. to ASD in relation to cyber security matters.

Supporting requirement 1. PSPF reporting model and template

Each entity must submit a report on security each financial year ...

...

Supporting requirement 2. Reporting security incidents

Each entity must report any significant or reportable security incidents at the time they occur to:

- a. the relevant authority ...
- b. other affected entities, and
- c. the Department of Home Affairs.

Supporting requirement 3. ASD cyber security survey

Each entity must complete ASD's annual cyber security survey.

Box 4: Protective Security Policy Framework, Policy 10 requirements**Core requirement**

Each entity must mitigate common cyber threats by:

- a. implementing the following mitigation strategies from the *Strategies to Mitigate Cyber Security Incidents*:
 - ...
 - viii. regular backups
- b. considering which of the remaining mitigation strategies from the *Strategies to Mitigate Cyber Security Incidents* need to be implemented to achieve an acceptable level of residual risk for their entity.

Appendix 4 ASD’s Cyber Security Guidelines — recommendations

Cyber Security Guidelines	Recommendations
<p>Guidelines for Cyber Security Incidents</p>	<p>Cyber security incidents are reported to ASD as soon as possible after they occur or are discovered.</p> <p>The types of cyber security incidents that should be reported to ASD include:</p> <ul style="list-style-type: none"> • suspicious activities, such as privileged account lockouts and unusual remote access activities; • compromise of sensitive or classified data; • unauthorised access or attempts to access a system; • emails with suspicious attachments or links; • denial-of-service attacks; and • ransomware attacks.
	<p>When a data spill occurs, data owners are advised and access to the data is restricted.</p>
	<p>When malicious code is detected, the following steps are taken to handle the infection:</p> <ul style="list-style-type: none"> • the infected systems are isolated; • all previously connected media used in the period leading up to the infection are scanned for signs of infection and isolated if necessary; • antivirus software is used to remove the infection from infected systems and media; and • if the infection cannot be reliably removed, systems are restored from a known good backup or rebuilt.
	<p>When handling and containing intrusions:</p> <ul style="list-style-type: none"> • legal advice is sought before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence; • system owners are consulted before allowing intrusion activity to continue on a system for the purpose of collecting further data or evidence; • planning and coordination of intrusion remediation activities are conducted on a separate system to that which has been compromised; • to the extent possible, all intrusion remediation activities are conducted in a coordinated manner during the same planned outage; and • following intrusion remediation activities, full network traffic is captured for at least seven days and analysed to determine whether malicious actors have been successfully removed from the system.

Cyber Security Guidelines	Recommendations
	<p>When gathering evidence following a cyber security incident, it is important that it is gathered in an appropriate manner and that its integrity is maintained.</p> <p>The integrity of evidence gathered during an investigation is maintained by investigators:</p> <ul style="list-style-type: none"> • recording all of their actions; • maintaining a proper chain of custody; and • following all instructions provided by relevant law enforcement agencies. <p>Following a cyber security incident being identified, an organisation's cyber security incident response plan should be enacted.</p>
Guidelines for System Monitoring	<p>A centralised event logging facility can be used to capture, protect and manage event logs from multiple sources in a coordinated manner. This may be achieved by using a Security Information and Event Management solution.</p> <p>A centralised event logging facility is implemented and:</p> <ul style="list-style-type: none"> • event logs are sent to the facility as soon as possible after they occur; • event logs are protected from unauthorised modification and deletion; and • an accurate time source is established and used consistently across systems to assist with identifying connections between events.
Guidelines for Cyber Security Roles	<p>The CISO contributes to the development, implementation and maintenance of business continuity and disaster recovery plans for their organisation to ensure that business-critical services are supported appropriately in the event of a disaster.</p>

Source: ASD's *Information Security Manual*.

Appendix 5 ASD’s Essential Eight Maturity Model

Essential Eight Maturity Model	Recommendations
Regular backups	Backups of data, applications and settings are: <ul style="list-style-type: none"> • performed and retained in accordance with business criticality and business continuity requirements; • synchronised to enable restoration to a common point in time; and • retained in a secure and resilient manner.
	Restoration of data, applications and settings from backups to a common point in time is tested as part of disaster recovery exercises.
	Unprivileged and privileged accounts (excluding backup administrator accounts): <ul style="list-style-type: none"> • cannot access backups belonging to other accounts; and • are prevented from modifying and deleting backups.

Source: ASD’s *Essential Eight Maturity Model*.

Appendix 6 PSPF Self-Assessment Maturity Model

PSPF Policies	Partial	Substantial	Full	Superior
<p>PSPF Policy 2 — Management structures and responsibilities</p>	<p>Security management structures and responsibilities are partially in place. Responsibility for designated security roles, protective security planning and management of security practices are basic and not consistent. Reporting is by exception with partial staff awareness of obligations. Incident response processes are informal and not centrally managed. Security is not consistently prioritised by leadership. Employees and contractors have some understanding of security obligations.</p>	<p>The CSO is appointed and most key security responsibilities are assigned. Security risk and incident reporting is occurring across the entity and response processes are centrally managed in the majority of cases. The importance of security and developing a strong security culture is substantially recognised by the leadership. The majority of personnel attend periodic security awareness and skills development training.</p>	<p>The CSO is empowered to investigate, respond to and report on security incidents. Clearly defined security roles and responsibilities exist with skilled personnel appointed by the CSO and empowered to make security decisions for their entity. A governance oversight function is established (where appropriate to entity size). Entity’s cycle of action, evaluation and learning is evident in response to security incidents. Personnel understand security incident reporting obligations with reporting processes published and accessible. Security is integral to the entity’s business and informs decision-making. Leadership is actively engaged and visibly prioritises good security practices with a strong security culture evident within the entity. Personnel’s participation in regular education programs that inform and assist their understanding of security-related processes and obligations is monitored.</p>	<p>Role of the CSO is highly visible and central to delivering on strategic business priorities and objectives. A security governance oversight function is operational. Security is embedded in entity operations, proactively managed and monitored, and is used to drive improvements which exceed mandatory security outcomes. Security procedures and practices are robust and of proven effectiveness. The CSO proactively ensures personnel resources are deployed to support the maintenance of effective protective security; appointing skilled personnel according to business needs. The CSO adopts a comprehensive, better practice approach to managing security incidents including investigating to determine root causes and inform security improvements and education programs. All personnel are trained annually on security policy and procedures and take responsibility for implementation within their area of responsibility. Security culture is underpinned by continuous improvement and accountability.</p>

PSPF Policies	Partial	Substantial	Full	Superior
PSPF Policy 4 — Security maturity monitoring	The entity partially monitors security maturity performance of its security capability and risk culture against the goals and strategic objectives identified in the entity security plan.	Security capability and risk culture is broadly addressed in the security plan. The performance and progress against the security plan's goals and strategic objectives is substantially monitored regularly.	Consistent and defined approach to monitoring the entity's security performance, which is tailored to the entity's risk environment. The entity has clearly defined security goals and objectives in the security plan. Performance is tracked and measured to assess security capability and risk culture maturity.	The entity proactively engages in ongoing monitoring and continuous improvement of security capability and culture through long-term planning to predict and prepare for security challenges. Performance data is captured and analysed to inform change and drive uplift, exceeding mandatory requirements.
PSPF Policy 5 — Reporting on security	The entity has partially met external reporting obligations to its portfolio minister, Home Affairs, other affected entities and ASD on cyber security matters. Reporting on the entity's achievement of security outcomes, implementation of core requirements, maturity of security capability, key risks to people, information and personnel and mitigation strategies to manage identified risks is basic and not consistent.	The entity substantially meets external reporting obligations to the portfolio minister, Home Affairs, other affected entities and ASD on cyber security matters. The entity's achievement of security outcomes, implementation of core requirements, maturity of security capability, key risks to people, information and personnel and mitigation strategies to manage identified risks is substantially captured in the annual security report.	The entity meets all external reporting obligations within required timeframes to the portfolio minister, Home Affairs, other affected entities and ASD on cyber security matters. The entity meets these obligations through effective reporting on achievement of security outcomes, implementation of core requirements, maturity of security capability, key risks to people, information and personnel and mitigation strategies. Key findings and trends are shared within the entity.	The entity exceeds reporting obligations and uses annual reporting to drive improvements, strengthen security culture and inform future planning, in line with better practice.

PSPF Policies	Partial	Substantial	Full	Superior
PSPF Policy 10 — Safeguarding data from cyber threats	The entity has partially implemented the Essential Eight Strategies to Mitigate Cyber Security Incidents, and has a reactive approach to considering the remaining strategies to protect the entity.	The entity has implemented the majority of the Essential Eight Strategies to Mitigate Cyber Security Incidents. The entity broadly understands and has substantially considered the remaining strategies necessary to protect the entity.	All Essential Eight Strategies to Mitigate Cyber Security Incidents have been fully implemented. The entity clearly understands and has considered the remaining strategies necessary to protect the entity.	The entity has fully implemented the Essential Eight Strategies to Mitigate Cyber Security Incidents, and considered and implemented other strategies relevant to the entity's risk environment, providing a superior level of protection against harm from identified cyber threats. Processes are regularly tested to ensure real-time response to potential cyber intrusions and emerging threats.

Source: ANAO summary of diagram in Department of Home Affairs' *PSPF Assessment Report 2022–23*, p. 4.