The Auditor-General
Auditor-General Report No.2 2024–25
Performance Audit

Defence’s Management of ICT Systems Security Authorisations

Department of Defence

Australian National Audit Office

ISSN 1036–7632 (Print)
ISSN 2203–0352 (Online)
ISBN 978-1-76033-959-3 (Print)
ISBN 978-1-76033-960-9 (Online)

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

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

Australian National Audit Office

Canberra ACT

11 September 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 Department of Defence. The report is titled *Defence's Management of ICT Systems Security Authorisations.* 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

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

Jarrad Hamilton
Hugh Balgarnie
Candy Chu
Sky Lo
Amy Willmott

Contents

Audit snapshot

Auditor-General Report No.2 2024–25

Defence's Management of ICT Systems Security Authorisations

Why did we do this audit?

- Malicious cyber activity represents a key risk for the Department of Defence (Defence).
- Protective Security Policy Framework (PSPF) Policy 11 outlines how ICT systems can be protected through authorisation activities to support the delivery of government business.
- This audit was conducted to provide assurance to the Parliament on Defence's arrangements for the management of its ICT systems authorisations.

Key facts

- The Defence Security Principles Framework (DSPF) requires that 'all Defence ICT systems must be authorised prior to processing, storing or communicating official information'.
- The DSPF provides for system authorisation decisions to be escalated to more senior personnel based on the system's assessed residual risk level.

What did we find?

- Defence's arrangements to manage the security authorisation of its ICT systems have been partly effective.
- Defence's arrangements for system authorisation have not been regularly reviewed and do not reflect current PSPF requirements.
- Defence's reporting did not comply with DSPF requirements, omitted key system authorisation data, and indicated a more optimistic outlook than was reflected in other Defence documentation.
- Defence did not comply with the PSPF and DSPF system authorisation requirements for the five case studies examined in the audit.

What did we recommend?

- There were eight recommendations to Defence aimed at improving: the review and update of assessment arrangements; training; the quality of supporting information; assurance and reporting arrangements; and compliance with authorisation requirements.
- Defence agreed to the eight recommendations.

285 days

was the average time to process system authorisations from September 2020 to September 2021.

5%

of Defence's ICT systems have been registered in Defence's ICT authorisation management system as at June 2024.

47%

of those ICT systems registered have been recorded as 'Expired' or 'No accreditation' as at August 2024.

Summary and recommendations

Background

1. The security of government information and communications technology (ICT) systems, networks and data supports Australia's social, economic and national security interests as well as the privacy of its citizens. Malicious cyber activity has been identified as a significant threat affecting Australians, exacerbated by low levels of cyber maturity across many Australian Government entities.[1]

2. The Department of Defence's (Defence's) mission and purpose is to defend Australia and its national interests in order to advance Australia's security and prosperity. Defence's 2022 Cyber Security Strategy states that 'Malicious cyber activity now represents one of Defence's most critical risks.'[2]

3. The Protective Security Policy Framework (PSPF) was introduced in 2010 to help Australian Government entities protect their people, information and assets, both at home and overseas. The PSPF sets out the government's protective security policy approach and is comprised of 16 core policies.[3] PSPF Policy 11 *Robust ICT systems* requires that:

> Entities **must** [emphasis in original] only process, store or communicate information and data on an ICT system that the determining authority (or their delegate) has authorised to operate based on the acceptance of the residual security risks associated with its operation.[4]
>
> When establishing new ICT systems, or implementing improvements to an existing system, the decision to authorise (or reauthorise) a system to operate **must** [emphasis in original] be based on the Information Security Manual's [ISM] six step risk-based approach for cyber security.[5]

4. Defence has established the Defence Security Principles Framework (DSPF) to support compliance with the requirements of the PSPF. The DSPF outlines Defence's requirements for ICT

1 Australian Government, *2023–2030 Australian Cyber Security Strategy* [Internet], 22 November 2023, p. 43, available from https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf [accessed 13 March 2024].

2 Department of Defence, *Defence Cyber Security Strategy* [Internet], 31 August 2022, p. 5, available from https://www.defence.gov.au/sites/default/files/2022-08/defence-cyber-security-strategy.pdf [accessed 13 March 2024].
A paper presented to Defence's Enterprise Business Committee in October 2021, seeking approval for the Cyber Security Strategy noted that: Defence's cyber security governance is 'fragmented and uncoordinated'; 'Defence's cyber security maturity ratings consistently fall below target scores'; and Defence has 'many legacy systems requiring disproportionate attention'.

3 Department of Home Affairs, *Protective Security Policy Framework* [Internet], available from https://www.protectivesecurity.gov.au/policies [accessed 3 April 2024].
The PSPF is not specifically legislated. The PSPF is underpinned by the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) requirements to govern an entity in a manner that is 'not inconsistent' with Australian Government policies and promote the proper use and management of public resources.

4 For systems with a classification of Top Secret, the Authorising Officer is the Director-General of the Australian Signals Directorate, or their delegate. As discussed at paragraph 1.25, the authorisation of Top Secret systems is outside the scope of this audit.

5 While PSPF Policy 11 and its associated requirements were introduced as part of a revision to the PSPF in 2018, the requirement for entities to authorise ICT systems based on the acceptance of residual risks has existed since the introduction of the ISM in 2009.

assessment and authorisation including that 'all Defence ICT systems must be authorised prior to processing, storing or communicating official information'.

Rationale for undertaking the audit

5. Through its 2022 Cyber Security Strategy, Defence has recognised that 'Malicious cyber activity now represents one of Defence's most critical risks.' Robust ICT systems protect the confidentiality, integrity and availability of the information and data that entities process, store and communicate. PSPF Policy 11 outlines how entities can safeguard ICT systems through assessment and authorisation activities to support the secure and continuous delivery of government business.

6. Questions regarding Defence's system authorisation process were raised at hearings of the Senate Foreign Affairs, Defence and Trade Legislation Committee in June 2021, including in relation to:

- Defence's use of provisional authorisations beyond 12 months for systems where security concerns have not been sufficiently addressed;
- deficiencies in Defence's processes for identifying and assessing risks as part of the authorisation process; and
- DSPF compliance with the Information Security Manual (ISM).

7. This audit was conducted to provide assurance to the Parliament on Defence's arrangements for the management of ICT systems security authorisations.[6]

Audit objective and criteria

8. The audit objective was to assess the effectiveness of the Department of Defence's arrangements to manage the security authorisation of its ICT systems.

9. To form a conclusion against this objective, the following high-level criteria were adopted.

- Does Defence have fit-for-purpose arrangements for the security authorisation of its ICT systems?
- Has Defence implemented its arrangements for the security authorisation of its ICT systems?

Engagement with the Australian Signals Directorate

10. 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.

6 The Hon Brendan O'Connor MP and Mr Tim Watts MP requested an audit into Defence's use of provisional authorisations on 5 June 2021. See Australian National Audit Office, *The use of provisional ICT accreditation within Defence* [Internet], 5 June 2021, available from https://www.anao.gov.au/work/request/the-use-provisional-ict-accreditation-within-defence [accessed 4 April 2024].

11. 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. The Australian Signals Directorate (ASD) has advised the ANAO that adversaries use publicly available information about cyber vulnerabilities to more effectively target their malicious activities.

12. The extent to which this report details the cyber security vulnerabilities of Defence 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 focusses on matters material to the audit findings against the objective and criteria.

Conclusion

13. Defence's arrangements to manage the security authorisation of its ICT systems have been partly effective. Systems have not been authorised in a timely manner and were assessed through processes that did not consistently comply with Protective Security Policy Framework (PSPF) requirements.

14. Defence's arrangements for the security authorisation of its ICT systems are partly fit for purpose. Defence's policies, frameworks and processes to support system assessment and authorisation have not been regularly reviewed or updated to align with PSPF and Defence Security Principles Framework (DSPF) requirements. These policy and process documents are internally inconsistent. Defence has not established training to ensure that key personnel involved in the authorisation process remain up-to-date with changing cyber security requirements in the Information Security Manual (ISM) and PSPF.

15. Defence has partly implemented arrangements for the security authorisation of its ICT systems. Defence's data on its system assessments and authorisations is incomplete and indicates that System Owner obligations to obtain and maintain authorisation of their systems are not being fulfilled.

16. There were deficiencies in relation to Defence's monitoring and reporting arrangements, including non-compliance with DSPF reporting requirements. Key information on the system authorisation status of Defence's systems was omitted from Defence's reporting, including not addressing a request from the Minister for Defence to include metrics in reporting on unapproved ICT systems within Defence. Defence's internal and external reporting on its assessments indicated a more optimistic outlook than was otherwise reflected in other internal Defence documentation. Across the ICT systems examined in case studies, deficiencies included: the absence of key data and mandatory security documentation; no evidence of assessment of control implementation; and deficiencies in the peer review process.

Supporting findings

Defence's arrangements for the security authorisation of its ICT systems

17. Defence has not appropriately maintained its policy and governance framework for the authorisation of its ICT systems. When the DSPF was implemented in July 2018, some sections

were not complete, with key authorisation roles listed but not defined for 13 of the 14 Defence Services and Groups listed. These roles remained undefined until a May 2024 review of the DSPF. Prior to the May 2024 update, DSPF Principle 23 and DSPF Control 23.1 had not been updated since July 2020. This meant that key changes to the mandatory requirements in PSPF Policies 10 and 11 between August 2020 and February 2022 — such as the introduction of the 'Essential Eight' and the ISM six-step process for system assessment and authorisation — were not reflected in the DSPF until 10 May 2024. (See paragraphs 2.3–2.25)

18. Directives, instructions, and policies issued by the Australian Defence Force (ADF) services for ICT authorisations for Army, Navy and Air Force systems contain provisions that are either not consistent with or not permitted by the requirements of the DSPF, or PSPF Policy 11. These provisions have allowed for exemptions to Defence's system authorisation process that are not permitted under the DSPF or PSPF. (See paragraphs 2.26–2.38)

19. A key supporting framework, the *Defence ICT Certification and Accreditation Framework* (DICAF) — developed to ensure consistency in the authorisation process for all Defence ICT systems that process, store or communicate official, sensitive or classified information — has been in draft since December 2015. As at May 2024, the DICAF remains incomplete with a placeholder remaining for a key section that was to be developed on the assessment and authorisation process. In response to shortcomings identified in the DICAF by an internal audit in May 2020, Defence developed a separate 'Assessment and Authorisation Framework' document in December 2021. The framework was approved by Defence's Chief Information Security Officer (CISO) in February 2024 and released in May 2024. (See paragraphs 2.39–2.51)

20. Defence does not have an up-to-date set of consolidated guidance to support the implementation of its framework in a consistent manner across the organisation. Defence's assessment and authorisation process guidance is internally inconsistent and a number of supporting templates have not been finalised or are outdated. Separate instructions, directives and policies exist for the Army, Navy and Air Force, which include some requirements that are inconsistent with Defence's assessment and authorisation process, the DSPF and PSPF. (See paragraphs 2.52–2.73)

21. Defence has not established training to ensure that Security Assessors remain up-to-date on evolving cyber security requirements, instead relying on peer review and Assessment Authority review to mitigate any 'deficiencies in knowledge'. Deficiencies were identified in Defence's implementation of the peer review process and Defence does not undertake assurance activities to monitor the extent to which training is completed. The absence of a formalised training approach to support the implementation of DSPF requirements for the assessment and authorisation of ICT systems creates a risk that systems are not being authorised as intended. Defence data on ICT system authorisations shows that 47 per cent of its systems have a status of either 'Expired' or 'No accreditation', indicating that System Owner obligations in respect to obtaining and maintaining the authorisation of their systems are not being met. (See paragraphs 2.74–2.93)

Implementation of arrangements for the security authorisation of Defence's ICT systems

22. Defence's data indicates that the obligations of System Owners to obtain and maintain the authorisation of their systems are not being fulfilled. (See paragraphs 3.5–3.26)

23. Defence self-assesses and reports annually on its compliance with PSPF Policy 11 and has established governance and internal reporting requirements for DSPF controls, including DSPF Control 23.1 *ICT Certification and Accreditation.* Deficiencies in Defence's reporting include that:

- Defence has not reported on the authorisation status of ICT systems at an enterprise level since 2018–19 in its PSPF and DSPF reporting (a key indicator of compliance against DSPF Control 23.1 and PSPF Policy 11);
- Defence's PSPF and DSPF reporting is not consistent with, and does not reflect, other information available within Defence on the assessment and authorisation of its ICT systems; and
- Defence has not complied with the DSPF requirement to provide individual Control Owner reports to the Defence Security Committee since 2019–20. (See paragraphs 3.27–3.68)

24. Defence has not briefed the minister on its ICT assessment and authorisation activities in the last three years. In September 2019, the minister requested that Defence include a metric on the reduction of unapproved systems in an 'ICT reform stream report'. Defence did not address this request. (See paragraphs 3.69–3.73)

25. Defence has not consistently complied with the requirements of its assessment and authorisation process. For example, for all five systems examined:

- key supporting data had not been entered in Defence's ICT authorisation management system, and mandatory security documentation had not been provided to the Security Assessors;
- Defence was unable to substantiate that document reviews and control implementation assessments took place; and
- there were shortcomings in the peer review process, including not identifying that mandatory security documentation was missing, and not identifying inaccuracies and errors in Risk Assessments. (See paragraphs 3.74–3.90)

26. There were instances where systems had been re-authorised based on the re-authorisation triggers in the DSPF. These re-authorisations were not always granted prior to authorisation expiry. (See paragraphs 3.91–3.100)

Recommendations

Recommendation no. 1
Paragraph 2.24

The Department of Defence ensure that DSPF roles and requirements for system assessment and authorisation are complete, current, and regularly reviewed for alignment with the PSPF and Group/Service appointments.

Department of Defence response: *Agreed.*

Recommendation no. 2
Paragraph 2.72

The Department of Defence conducts a review of, and updates, its assessment and authorisation process documentation to ensure:

(a) alignment with current DSPF and PSPF requirements;

(b) consistency across all internal guidance documents, including those developed by the ADF Services; and

(c) that any internal inconsistencies within individual guidance documents are eliminated.

Department of Defence response: *Agreed.*

Recommendation no. 3
Paragraph 2.89

The Department of Defence:

(a) implements improved training and awareness raising activities to ensure that key personnel involved in the assessment and authorisation process are aware of their obligations under the PSPF and DSPF, and remain up-to-date with evolving cyber security requirements; and

(b) implements a framework to monitor and report on the completion of training and awareness raising activities.

Department of Defence response: *Agreed.*

Recommendation no. 4
Paragraph 3.25

The Department of Defence develops and implements processes to ensure that information entered into its ICT authorisation management system is complete, accurate, and supports effective monitoring of ICT system authorisations.

Department of Defence response: *Agreed.*

Recommendation no. 5
Paragraph 3.45

The Department of Defence:

(a) implement enterprise-wide assurance arrangements to support the effective implementation of DSPF system authorisation requirements; and

(b) implement arrangements to ensure that deficiencies and non-compliance identified through Service assurance activities relating to system authorisations are addressed and rectified.

Department of Defence response: *Agreed.*

Recommendation no. 6
Paragraph 3.67

The Department of Defence implement arrangements to ensure reporting to senior Defence leadership on compliance with system authorisation requirements under the PSPF and DSPF is comprehensive, accurate, and based on available data.

Department of Defence response: *Agreed.*

Recommendation no. 7
Paragraph 3.72

The Department of Defence:

(a) ensures that relevant ministers are provided with timely and accurate advice on key issues and risks relating to Defence's ICT security authorisations and its compliance with the PSPF; and

(b) provides regular (at least annual) updates to relevant ministers to support oversight for improvements to its

assessment and authorisation policies, frameworks and processes.

Department of Defence response: *Agreed.*

Recommendation no. 8
Paragraph 3.98

The Department of Defence implements arrangements to ensure that PSPF requirements, DSPF requirements and Defence's assessment and authorisation process are complied with, including:

(a) ensuring that all required documentation has been completed prior to system assessment and authorisation;

(b) documenting the approval and review of mandatory supporting documentation;

(c) conducting and documenting assessments of the implementation and effectiveness of controls and provisional authorisation conditions against all relevant ISM and DSPF controls; and

(d) ensuring systems are proactively monitored against the conditions for re-authorisation.

Department of Defence response: *Agreed.*

Summary of the Department of Defence's response

27. The proposed audit report was provided to the Department of Defence. Defence's summary response is provided below, and its full response is included at Appendix 1. Improvements observed by the ANAO during the course of this audit are listed in Appendix 2.

> Defence welcomes the Auditor-General Report: *Defence's Management of ICT Security Authorisation*. Defence agrees to the eight recommendations aimed at improving Defence's Cyber Security Assessment and Authorisation Framework to more effectively govern and monitor the authorisation of ICT systems and networks and control cyber-related ICT risk.
>
> Defence is committed to strengthening and standardising our approach to safeguarding data from cyber threats and ensuring the secure operation of our ICT systems to protect the continuous delivery of Defence outcomes. Defence is currently reviewing its Cyber Security Assessment and Authorisation Framework, along with the associated policies, practices and processes, as part of Defence's wider initiative to uplift cyber security governance and its cyber risk management framework. This includes an overhaul of several pertinent Defence Security Principles Framework policies, which are undergoing review, along with a program to drive Essential 8 Maturity.

Key messages from this audit for all Australian Government entities

28. 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

- Policy and guidance documentation should be kept up-to-date, especially when it relates to activities to manage key entity risks. Periodic review of documentation helps maintain its fitness-for-purpose and alignment with Commonwealth standards.

Performance and impact measurement

- Accurate and transparent monitoring and reporting on compliance supports effective decision-making and accountability. Monitoring and reporting should be supported by data that is accurate and complete.

Audit findings

1. Background

Introduction

1.1 The security of government information and communications technology (ICT) systems, networks and data supports Australia's social, economic and national security interests as well as the privacy of its citizens. Malicious cyber activity has been identified as a significant threat affecting Australians, exacerbated by low levels of cyber maturity across many Australian Government entities.[7]

1.2 The Australian Signals Directorate (ASD) *Cyber Threat Report 2022–23* identified that:

> the regional strategic environment continues to deteriorate, which is reflected in the observable activities of some state actors in cyberspace. In this context, these actors are increasingly using cyber operations as the preferred vector to build their geopolitical competitive edge, whether it is to support their economies or to underpin operations that challenge the sovereignty of others. In the Australian Security Intelligence Organisation's Annual Report 2021–22, espionage and foreign interference was noted to have supplanted terrorism as Australia's principal security concern.[8]

1.3 The Department of Defence's (Defence's) mission and purpose is to defend Australia and its national interests in order to advance Australia's security and prosperity. Defence's *2022–23 Annual Report* states that, to enable the warfighting capabilities of the Australian Defence Force (ADF) globally, it is supported by one of the largest and most complex ICT environments in the nation.[9]

1.4 Defence's *2022 Cyber Security Strategy* states that 'Malicious cyber activity now represents one of Defence's most critical risks.'[10] This risk was reflected in the 2023 *Defence Strategic Review*, which found that limited workforce availability had resulted in project slippage and insufficient ADF and Australian Public Service (APS) staff to manage heavily outsourced ICT functions. The review recommended:

- the appointment of a 'dedicated senior official for Chief Information Officer Group (CIOG) capability management leadership and a dedicated senior official accountable for [Defence's] secret network', and rebalancing of the CIOG workforce to a 60:40 APS- and ADF-to-contractor ratio;
- enhancement of Defence's cyber security arrangements in collaboration with ASD; and

7 Australian Government, *2023–2030 Australian Cyber Security Strategy* [Internet], 22 November 2023, p. 43, available from https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf [accessed 13 March 2024].

8 Australian Signals Directorate, *ASD Cyber Threat Report 2022–23* [Internet], 14 November 2023, p. 27, available from https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf [accessed 13 March 2024].

9 Department of Defence, *2022–23 Defence Annual Report* [Internet], 18 September 2023, p. 130, available from https://www.defence.gov.au/sites/default/files/2023-10/Defence-Annual-Report-2022-23.pdf [accessed 13 March 2024].

10 Department of Defence, *Defence Cyber Security Strategy* [Internet], 31 August 2022, p. 5, available from https://www.defence.gov.au/sites/default/files/2022-08/defence-cyber-security-strategy.pdf [accessed 13 March 2024].

A paper presented to Defence's Enterprise Business Committee in October 2021, seeking approval for the Cyber Security Strategy noted that: Defence's cyber security governance is 'fragmented and uncoordinated'; 'Defence's cyber security maturity ratings consistently fall below target scores'; and Defence has 'many legacy systems requiring disproportionate attention'.

- increasing Defence's cyber security operations capability in CIOG and decommissioning legacy systems and platforms.[11]

1.5 The Australian Government agreed to the recommendations.

Protective Security Policy Framework

1.6 The Protective Security Policy Framework (PSPF) was introduced in 2010 to help Australian Government entities protect their people, information and assets, both at home and overseas. The PSPF sets out the government's protective security policy approach and is comprised of 16 core policies.[12] Under the PSPF, all entities are required to develop their own protective security policies and procedures. PSPF Policy 10 *Safeguarding data from cyber threats* and Policy 11 *Robust ICT systems* outline how entities can safeguard their ICT systems and mitigate their exposure to cyber security risks.

PSPF Policy 10 — Safeguarding data from cyber threats

1.7 PSPF Policy 10 *Safeguarding data from cyber threats* requires entities to mitigate common security threats by implementing eight essential mitigation strategies (the Essential Eight).[13] Prior to February 2022, only four of the strategies were mandatory. Entities must implement Maturity Level 2 for each of the eight strategies to be compliant.[14] Defence's system authorisation process requires consideration of the Essential Eight as part of supporting security documentation (see paragraphs 2.58–2.59).

PSPF Policy 11 — Robust ICT systems

1.8 PSPF Policy 11 *Robust ICT systems* requires that entities ensure the secure operation of their ICT systems to safeguard their information and data and the continuous delivery of government business by applying the Information Security Manual's (ISM) cyber security principles during all stages of the lifecycle of each system. Specifically, PSPF Policy 11 requires that:

> Entities **must** [emphasis in original] only process, store or communicate information and data on an ICT system that the determining authority (or their delegate) has authorised to operate based on the acceptance of the residual security risks associated with its operation.[15]

---

11 Australian Government, *National Defence: Defence Strategic Review 2023* [Internet], 23 April 2023, pp. 82–83, available from https://www.defence.gov.au/about/reviews-inquiries/defence-strategic-review [accessed 13 March 2024].

12 Department of Home Affairs, *Protective Security Policy Framework* [Internet], available from https://www.protectivesecurity.gov.au/policies [accessed 3 April 2024].
The PSPF is not specifically legislated. The PSPF is underpinned by the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) requirements to govern an entity in a manner that is 'not inconsistent' with Australian Government policies and promote the proper use and management of public resources.

13 Developed by ASD to help organisations mitigate cyber security incidents, the Essential Eight mitigation strategies are: application control; patch applications; configure Microsoft Office macro settings; user application hardening; restrict administrative privileges; patch operating systems; multi-factor authentication and regular backups. ASD's 'Essential Eight Maturity Model', is designed to assist organisations to implement the Essential Eight. See https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model [accessed 24 October 2023].

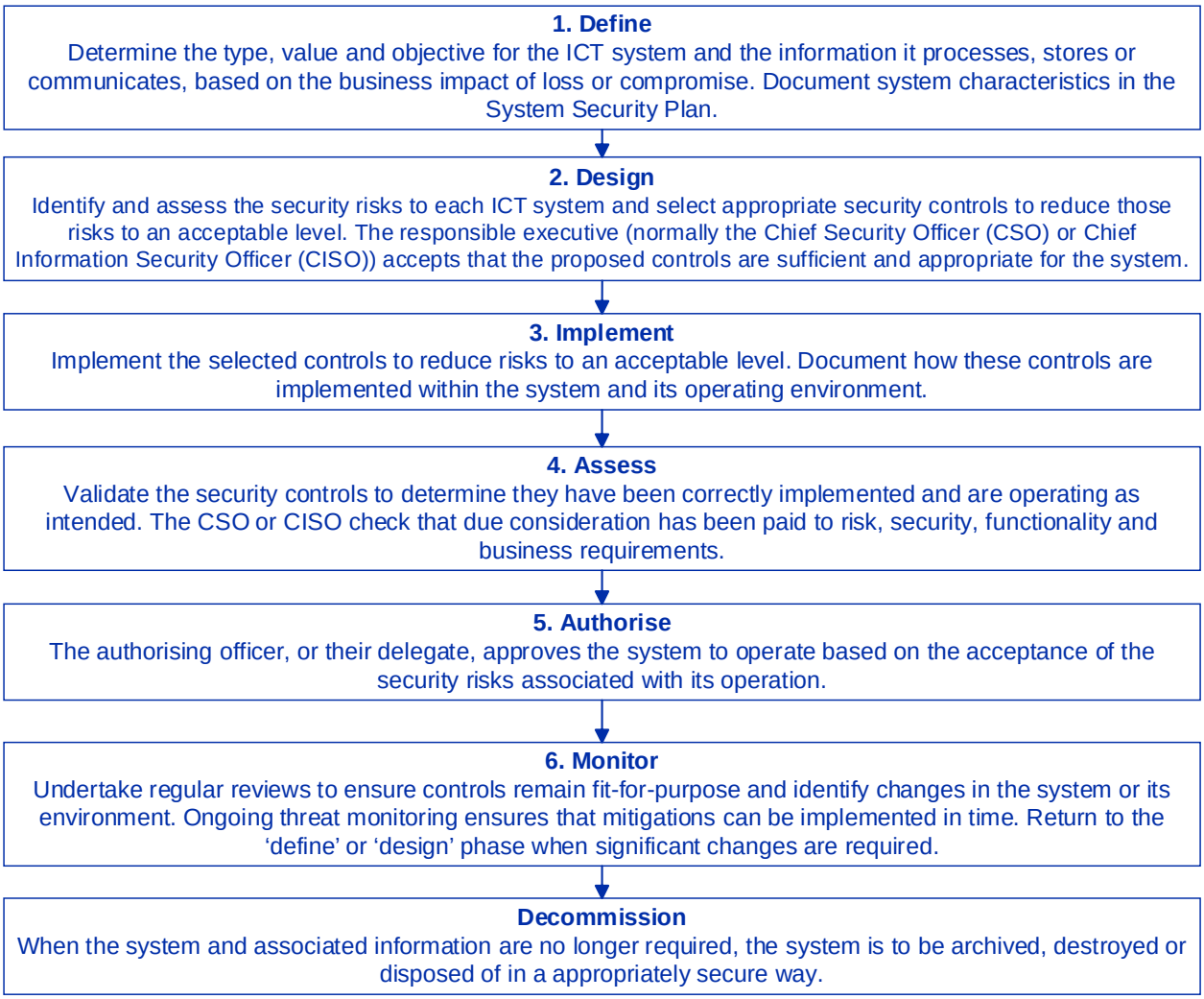
14 The Essential Eight Maturity Model defines four maturity levels — Maturity Level Zero to Maturity Level 3.

15 For systems with a classification of Top Secret, the Authorising Officer is the Director-General of ASD, or their delegate. As discussed at paragraph 1.25, the authorisation of Top Secret systems is outside the scope of this audit.

When establishing new ICT systems, or implementing improvements to an existing system, the decision to authorise (or reauthorise) a system to operate **must** [emphasis in original] be based on the Information Security Manual's six step risk-based approach for cyber security.[16]

1.9 The ISM six-step process is outlined in Figure 1.1 below.

Figure 1.1: ISM six-step risk-based process



Source: ANAO analysis of PSPF Policy 11.

1.10 Prior to August 2020, PSPF Policy 11 used the terms 'certification' and 'accreditation' and referred to the key decision-making roles for certification and accreditation as the 'certification authority' and 'accreditation authority' respectively. Since August 2020, PSPF Policy 11 refers to 'certification' as 'assessment' and 'accreditation' as 'authorisation'. The key decision-making roles for assessment and authorisation have been defined in PSPF Policy 11 as the Chief Security Officer (CSO) or Chief Information Security Officer (CISO) and 'authorising officer' respectively.[17]

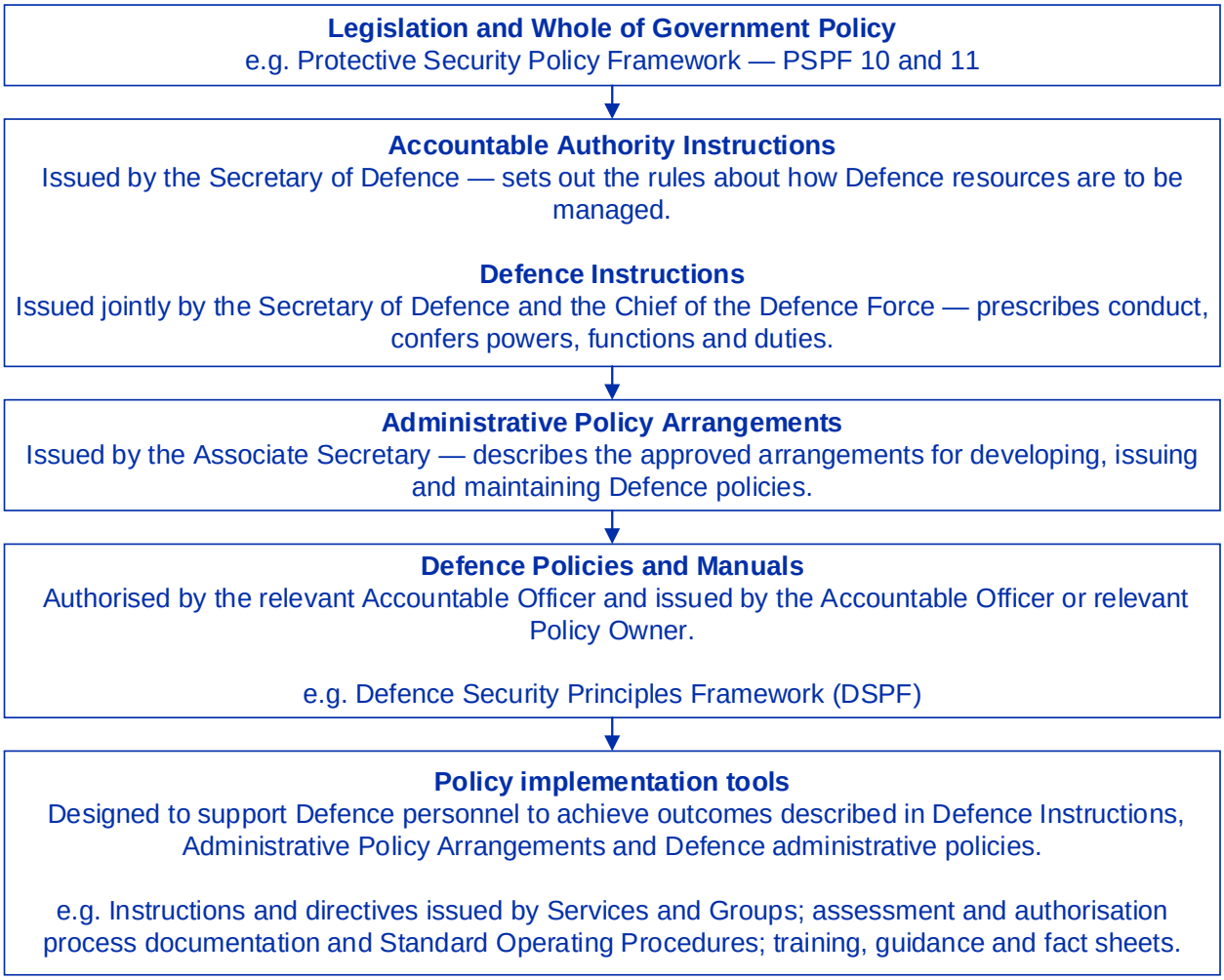
16 While PSPF Policy 11 and its associated requirements were introduced as part of a revision to the PSPF in 2018, the requirement for entities to authorise ICT systems based on the acceptance of residual risks has existed since the introduction of the ISM in 2009.

17 This report uses the terms 'assessment' and 'authorisation' to refer to the authorisation process, unless quoting from Defence documentation.

ICT system authorisations in Defence

1.11 Defence has developed Administrative Policy Arrangements which establish the authority and hierarchy for Defence documents. This hierarchy, and its relationship to key documents referred to throughout this report are outlined in Figure 1.2.

Figure 1.2: Hierarchy of Defence documents



Source: ANAO analysis of Defence's Administrative Policy Arrangements.

Defence Security Principles Framework

1.12 Defence has established the Defence Security Principles Framework (DSPF) to support compliance with the requirements of the PSPF. DSPF Principle 23, which is supported by Control 23.1 *ICT Certification and Accreditation,* outlines Defence's requirements for ICT assessment and authorisation including that:

- all Defence ICT systems must be authorised prior to processing, storing or communicating official information;
- the authorising officer is based on the level of assessed system risk; and
- ICT systems are to be re-authorised under various conditions including when: new or emerging threats are identified; a cyber security incident occurs; changes to the certified system architecture occur; or the system's authorisation expires.

1.13 The DSPF is supported by directives and instructions issued by Defence's Services and Groups, discussed further at paragraphs 2.26–2.38.

Defence Cyber and Information Assurance Branch

1.14 The Defence Cyber and Information Assurance Branch (DCIAB) sits within Defence's Cyber Command[18] and is responsible for ensuring cyber security risks are effectively quantified and managed across Defence systems and networks. This includes the provision of ICT system assessment and authorisation services conducted by the Cyber Security Assessments and Authorisation (CSAA) Directorate within DCIAB. Defence's CISO is the head of DCIAB.[19]

1.15 Between 2020–21 and 2022–23 DCIAB's expenditure increased by 234 per cent. The number of contractors engaged by DCIAB increased by 72 per cent and the number of APS and ADF personnel increased by 3 per cent over the same three-year period.

Defence ICT systems

1.16 Defence defines a 'system' in its 'Cyber Security Assessment and Authorisation Framework' as:

> a single or a group of interacting Information and Communication Technology (ICT) hardware and/or software components that enable users to accomplish a task (i.e. that stores, processes or communicates information). Systems may include other systems.

1.17 In September 2021, Defence commenced an ICT inventory project to develop a 'comprehensive knowledge base of all current Defence portfolio ICT systems, networks, applications and services' (see paragraphs 3.7–3.11).

1.18 Approximately 48 per cent of the systems that have been identified through the inventory project are systems that 'manage the creation, processing, presentation and storage of information' and need to be authorised in accordance with PSPF Policy 11. Of these systems, 5 per cent were recorded in Defence's system for managing ICT authorisations as at June 2024. The data recorded in Defence's ICT authorisation management system is not complete or accurate (see paragraphs 3.15–3.26).

Rationale for undertaking the audit

1.19 Through its *2022 Cyber Security Strategy*, Defence has recognised that 'Malicious cyber activity now represents one of Defence's most critical risks.' Robust ICT systems protect the confidentiality, integrity and availability of the information and data that entities process, store and communicate. PSPF Policy 11 outlines how entities can safeguard ICT systems through assessment and authorisation activities to support the secure and continuous delivery of government business.

1.20 Questions regarding Defence's system authorisation process were raised at hearings of the Senate Foreign Affairs, Defence and Trade Legislation Committee in June 2021, including in relation to:

18 Cyber Command, formerly known as the Cyber Warfare Division, was established in March 2024, and sits within Defence's Joint Capabilities Group.

19 Prior to December 2023, DCIAB was called the ICT Security Branch (ICTSB) and prior to July 2023, the branch was located within the Chief Information Officer Group (CIOG). The restructure was undertaken as part of implementing recommendations from the Defence Strategic Review.

- Defence's use of provisional authorisations beyond 12 months for systems where security concerns have not been sufficiently addressed;
- deficiencies in Defence's processes for identifying and assessing risks as part of the authorisation process; and
- DSPF compliance with the ISM.

1.21 This audit was conducted to provide assurance to the Parliament on Defence's arrangements for the management of ICT systems security authorisations.[20]

Audit approach

Audit objective, criteria, and scope

1.22 The audit objective was to assess the effectiveness of the Department of Defence's arrangements to manage the security authorisation of its ICT systems.

1.23 To form a conclusion against this objective, the following high-level criteria were adopted.

- Does Defence have fit-for-purpose arrangements for the security authorisation of its ICT systems?
- Has Defence implemented its arrangements for the security authorisation of its ICT systems?

1.24 The audit scope included examination of the arrangements Defence has in place to identify, assess, and mitigate or accept ICT system security risks, and examination of Defence's implementation of its arrangements. ICT systems included in the scope of the audit are systems that process, store or communicate official information.

1.25 The scope did not include examination of the authorisation of Top Secret ICT systems. These authorisations are done by the Australian Signals Directorate (ASD), not Defence.

Audit methodology

1.26 The audit methodology included discussions with relevant Defence officials and an examination and analysis of Defence records.

1.27 The audit was open to contributions from the public. The ANAO did not receive any submissions.

1.28 The audit was conducted in accordance with ANAO Auditing Standards at a cost to the ANAO of approximately $504,803.

1.29 The team members for this audit were Jarrad Hamilton, Hugh Balgarnie, Candy Chu, Sky Lo, and Amy Willmott.

20 The Hon Brendan O'Connor MP and Mr Tim Watts MP requested an audit into Defence's use of provisional authorisations on 5 June 2021. See Australian National Audit Office, *The use of provisional ICT accreditation within Defence* [Internet], 5 June 2021, available from https://www.anao.gov.au/work/request/the-use-provisional-ict-accreditation-within-defence [accessed 4 April 2024].

2. Defence's arrangements for the security authorisation of its ICT systems

Areas examined

This chapter examines whether the Department of Defence (Defence) has fit for purpose arrangements in place for the security authorisation of its ICT systems.

Conclusion

Defence's arrangements for the security authorisation of its ICT systems are partly fit for purpose. Defence's policies, frameworks and processes to support system assessment and authorisation have not been regularly reviewed or updated to align with Protective Security Policy Framework (PSPF) and Defence Security Principles Framework (DSPF) requirements. These policy and process documents are internally inconsistent. Defence has not established training to ensure that key personnel involved in the authorisation process remain up-to-date with changing cyber security requirements in the Information Security Manual (ISM) and PSPF.

Areas for improvement

The ANAO made three recommendations aimed at: reviewing and updating the DSPF and Defence's assessment and authorisation process; and implementing improved training to ensure key assessment and authorisation personnel are aware of their obligations under the PSPF and DSPF.

2.1 Protective Security Policy Framework (PSPF) Policy 11 *Robust ICT systems* mandates that entities must only process, store or communicate information and data on an ICT system that the 'determining authority' has authorised to operate based on the acceptance of the residual security risks associated with its operation. The decision to authorise a system must be based on the Information Security Manual's (ISM's) six-step risk-based approach to cyber security (see Figure 1.1).

2.2 Since February 2022, PSPF Policy 10 *Safeguarding data from cyber threats* has required entities to mitigate common security threats by implementing eight essential mitigation strategies, known as the 'Essential Eight' (see footnote 13). Prior to this update, only four of the strategies were mandatory. Defence has established policies to support PSPF Policy 10 and 11 through ICT assessment and authorisation in the Defence Security Principles Framework (DSPF) and Service-level directives, instructions, and policies.

Has Defence established an appropriate policy and governance framework for the security authorisation of its ICT systems?

Defence has not appropriately maintained its policy and governance framework for the authorisation of its ICT systems. When the DSPF was implemented in July 2018, some sections were not complete, with key authorisation roles listed but not defined for 13 of the 14 Defence Services and Groups listed. These roles remained undefined until a May 2024 review of the DSPF. Prior to the May 2024 update, DSPF Principle 23 and DSPF Control 23.1 had not been updated since July 2020. This meant that key changes to the mandatory requirements in PSPF Policies 10 and 11 between August 2020 and February 2022 — such as the introduction of the

'Essential Eight' and the ISM six-step process for system assessment and authorisation — were not reflected in the DSPF until 10 May 2024.

Directives, instructions, and policies issued by the Australian Defence Force (ADF) services for ICT authorisations for Army, Navy and Air Force systems contain provisions that are either not consistent with or not permitted by the requirements of the DSPF, or PSPF Policy 11. These provisions have allowed for exemptions to Defence's system authorisation process that are not permitted under the DSPF or PSPF.

A key supporting framework, the *Defence ICT Certification and Accreditation Framework* (DICAF) — developed to ensure consistency in the authorisation process for all Defence ICT systems that process, store or communicate official, sensitive or classified information — has been in draft since December 2015. As at May 2024, the DICAF remains incomplete with a placeholder remaining for a key section that was to be developed on the assessment and authorisation process. In response to shortcomings identified in the DICAF by an internal audit in May 2020, Defence developed a separate 'Assessment and Authorisation Framework' document in December 2021. The framework was approved by Defence's Chief Information Security Officer (CISO) in February 2024 and released in May 2024.

Defence Security Principles Framework

2.3 Defence has established its primary policy requirements for ICT system assessment and authorisation through the DSPF. The DSPF was introduced in July 2018, replacing the Defence Security Manual (DSM). The introduction of the DSPF reflected Defence's stated transition from a 'compliance model of security management under the Defence Security Manual' to a 'principles based approach' under the DSPF. The DSPF states that this approach:

- Allows all parts of Defence to manage security within their operational context and constraints. This recognises the best security decisions are made in accordance with agreed principles, with a desired outcome in mind.
- Ensures the most appropriate people are setting security requirements. Those who know their business are best placed to set security standards and requirements for that aspect of Defence business.

2.4 Under DSPF Principle 23, Control 23.1 *ICT Certification and Accreditation* requires that 'All Defence ICT systems must be accredited prior to processing, storing or communicating Official information' and outlines: Defence's high-level process for assessment and authorisation, including Authorising Officer levels, which are aligned to risk ratings; an assessment and authorisation flowchart; and requirements for re-authorising ICT systems.

2.5 The DSM included similar authorisation requirements to the DSPF, but also included additional requirements that were not retained after the introduction of the DSPF, such as:

- annual review and monitoring of authorised ICT systems (see footnote 73);
- mandatory training for Authorising Officers (see paragraph 2.74);
- recording the extent of a system's compliance against all applicable 'must' and 'should' statements contained in the ISM, as part of the assessment process;
- the issuing of a dispensation (provisional authorisation) for a specified timeframe by the relevant Group Head or Service Chief in exceptional circumstances;

- the closure of a system and withdrawal of provisional authorisation where there is a failure to meet the conditions of the authorisation within the specified timeframe; and
- not using the provisional authorisation process 'as a means to circumvent the proper application' of the authorisation process.

2.6 The DSPF states that it is a 'flexible policy framework' and that 'DSPF documents will be reviewed and updated as necessary'. Prior to 10 May 2024, DSPF Principle 23 was last approved by the Chief Security Officer in July 2020, and had not been updated to reflect amendments made to PSPF Policy 11 in August 2020, including mandating the ISM's six-step authorisation process and changes to PSPF language.[21] An updated version of DSPF Principle 23 and Control 23.1, which reflects the six-step process and updated PSPF language, was approved by the Chief Information Security Officer (CISO) on 10 May 2024.

2.7 DSPF Control 20.1 *Information Systems Lifecycle Management* was last reviewed in July 2020 and only recognises four of the ISM's Essential Eight strategies as being mandatory. This is not in line with the requirements of PSPF Policy 10, which were amended in February 2022 and state that '[t]o meet the minimum requirements established under the PSPF maturity model, entities must implement Maturity Level Two for each of the eight essential mitigation strategies'.

DSPF roles and responsibilities

2.8 Roles and responsibilities for personnel involved in the assessment and authorisation process are primarily established in the DSPF through Control 20.1 *Information Systems Lifecycle Management* and Control 23.1 *ICT Certification and Accreditation.*

2.9 Prior to updates to the DSPF in May 2024, the Control Owner for these controls was Defence's IT Security Advisor (ITSA), which is an Executive Level 2 (EL2) position.[22] The DSPF states that Controls Owners are 'An SES or ADF [Australian Defence Force] Star Rank Officer assigned accountability and authority to manage a specific defence security risk. These will be derived from the DSPF Principles and Expected Outcomes. The relevant Control Owner in each instance may be a Group Head or Service Chief, or a more appropriate subordinate'. As at March 2024, the only controls in the DSPF delegated below SES or ADF Star Rank Officer level were controls delegated to the ITSA. The CISO (an SES Band 1 Officer) has been appointed as the Control Owner in Defence's May 2024 updated DSPF Control 23.1.The ITSA no longer has a defined role in the updated DSPF Control 23.1.

2.10 Table 2.1 outlines the roles and responsibilities as established in the July 2020 approved DSPF controls (which applied at the time this audit commenced in November 2023).

21 As discussed at paragraph 1.10, updates to PSPF Policy 11 in August 2020 included replacing the term 'certification' with 'assessment' and 'accreditation' with 'authorisation'. This audit report uses the terms 'assessment' and 'authorisation' to refer to the authorisation process, unless quoting from Defence documentation.

22 In January 2020, following an organisational restructure in the Chief Information Officer Group, Defence appointed a new CISO at the SES Band 1 level. Prior to this, the CISO was a SES Band 2 officer. The role of ITSA, who reports to the CISO was adjusted accordingly from an SES Band 1 position to an EL2 position.

Table 2.1: ICT security authorisation roles and responsibilities, as per July 2020 DSPF

Role title (and classification)	Role description
Chief Information Security Officer (CISO) Classification: SES Band 1	• Manage and report on authorisation activities across Defence. • Maintain an effective ICT assessment and authorisation framework for Defence in accordance with Government expectations, Defence policy and the Defence ICT security strategy.[a] • The CISO is also the Assistant Secretary of the ICT Security Branch (ICTSB), now called the Defence Cyber and Information Assurance Branch (DCIAB).[b] • The DSPF states that the Assistant Secretary fulfils the role of 'Certification Authority' (discussed below) for the majority of Defence systems classified Secret or below.[c]
Information Technology Security Advisor (ITSA) Classification: EL2	• The ITSA is located within the DCIAB and is the 'Control Owner' for Control 23.1. • Coordinate ICT assessment and authorisation functions to a standard that meets Government expectations. • Approve subordinate security controls, processes or instructions relevant to their control.[d] • Manage and report on assessment activities across Defence. • Provide appropriate assurance and reporting to the Defence Security Committee (DSC) and the Chief Security Officer. • Endorse Assessment Authorities (Certification Authorities) and Security Assessors (Certification Consultants). • Maintain visibility of certified systems and associated recommendations made to Authorising Officers.
Accreditation Authority Classification: EL1/O4 to SES3/3-Star. Referred to as 'Authorising Delegate' in the updated May 2024 DSPF Control 23.1. Referred to as 'Authorising Officer' in PSPF Policy 11 and in this report.	• The Authorising Officer is located within the relevant business area for the system being authorised. The Authorising Officer is determined on an individual system basis according to assessed risk and the 'escalation thresholds' outlined in Table 2.2. • Responsible for formal recognition, approval and acceptance of the risks to a system, and approving a system into operation. • Confirm that system assessment has been conducted to a suitable standard. • Maintain visibility of all systems awarded authorisation and their associated re-authorisation schedules. • Report authorisation outcomes to the CISO. • Where required, delegate risk acceptance to the Cyber Security Executive (CSE) or Cyber Security Advisor (CSA) within their Group/Service.
Certification Authority Referred to as 'Assessment Authority' in this report (and in the updated May 2024 DSPF Control 23.1). Classification: EL2/O5 to SES3/3-Star.	• The Assessment Authority is the CISO (within DCIAB) for all Defence systems except those belonging to Air Force.[e] • Identify and appoint a suitably qualified security assessor to conduct a security assessment (if required).[f] • Award system 'certification' by endorsing the residual risk identified through a security assessment. • Provide recommendations on authorisation to the Authorising Officer, including: whether to accept the residual risk; whether to issue a full or

Role title (and classification)	Role description
	provisional authorisation; any conditions that should be placed on the approval; any remediation activities that must be completed during the approval period (for provisional authorisations); and the duration of the authorisation period. • Report security assessment outcomes to the ITSA.[g]
Certification Consultant Referred to as 'Security Assessor' in this report (and the updated May 2024 DSPF Control 23.1).	• Security Assessors are located within DCIAB. • Provide advice and guidance to the System Owner throughout all phases of system development on strategies to reduce risk to an acceptable level. • Maintain independence throughout the assessment process. • Conduct security assessments against current security policy and standards to assess residual risk and provide a Risk Assessment to the Assessment Authority (Certification Authority) which articulates risks and recommendations. • Maintain evidence of activities conducted during a security assessment.
System Owner	• The System Owner sits within the relevant business area of the system for which they are responsible. • Obtain and maintain authorisation of their systems. • Assess the system's Business Impact Level (BIL). • Develop relevant security documentation for their system. • Maintain independence from the Authorising Officer.

Note a: This responsibility is established under Control 19.1 *Information Systems (Logical) Security.*

Note b: As discussed at footnote 19, ICTSB transitioned to DCIAB as part of a restructure in December 2023.

Note c: Since 2018, the DSPF has established the Commanding Officer of Air Force's 462 Squadron as the Assessment (Certification) Authority for Air Force standalone systems. PSPF Policy 11 stipulates the Chief Security Officer (CSO) or CISO as the responsible officer for ensuring that the assessment process has given due consideration to 'risk, security, functionality and business requirements'. Prior to being updated in August 2020, PSPF Policy 11 established the CSO (or delegated security advisor) as the 'Certification Authority'. Defence advised the ANAO in June 2024 that the Commanding Officer of 462 Squadron was delegated the Authorising Officer role from Air Force's Provost Marshall (the Air Force's Single Service Security Authority) 'well before the creation of the PSPF / DSPF and the CSO role. This delegation is understood to have been grandfathered into the DSPF in 2018 from the Defence Security Manual.'

Note d: Defence advised the ANAO in May 2024 that no formal Control Owner approval has been provided for Defence's assessment and authorisation process (discussed at paragraphs 2.53–2.73), Deputy Chief of Army Directive 01-20 — Army ICT Security Plan (discussed at paragraphs 2.27–2.30), the Navy Cyberworthiness policy (discussed at paragraphs 2.31–2.32) or Air Force instruction AFSI (OPS) 05-02 (discussed at paragraphs 2.33–2.35). Defence further advised in June 2024 that Control Owner approval was not provided for Air Command Standing Instruction AC SI(OPS) 05-50 (discussed at paragraph 2.36).

Note e: The 'Assessment Authority' role is not specifically outlined in PSPF Policy 11. As noted at Note c, PSPF Policy 11 stipulates the CSO or CISO as the responsible officer for ensuring that the assessment process has given due consideration to 'risk, security, functionality and business requirements'.

Note f: The DSPF states that whether an outside consultant will be required 'will be dependent on the Group/Service and the Protective Marking of the material to be processed, stored and communicated on the system'.

Note g: Defence advised the ANAO in August 2024 that this requirement was included to ensure that the assessment of systems outside of the CISO's assessment responsibilities (such as Air Force systems) were reported to the ITSA.

Source: ANAO analysis of the DSPF.

2.11 The DSPF also establishes Authorising Officer 'escalation thresholds' for system authorisation, outlined in Table 2.2.

Table 2.2: DSPF system authorisation escalation thresholds per July 2020 DSPF Control 23.1

Risk rating	Authorising officer — Chief Information Officer Group (CIOG) managed or connected systems	Authorising officer — Group/Service managed systems
Low	Minimum SES Band 1 or 1 Star.	EL1 or O4[a] employed in a relevant ICT security role.
Moderate	Minimum SES Band 1 or 1 Star.	EL2 or O5[b] employed in a relevant ICT security role.
Significant	Minimum SES Band 1 or 1 Star.	Appointed Cyber Security Advisor (CSA) or the ITSA in the event that a CSA has not been appointed.
High	SES Band 2 or 2 Star.	Appointed Cyber Security Executive (CSE) or the CISO in the event that a CSE has not been appointed.
Extreme	SES Band 3 or 3 Star.	Appointed Group Head or Service Chief.

Note a: O4 rank is equivalent to a Lieutenant Commander (Navy), Major (Army), or Squadron Leader (Air Force).

Note b: O5 rank is equivalent to a Commander (Navy), Lieutenant Colonel (Army), or Wing Commander (Air Force). The updated DSPF Control 23.1, approved by the CISO in May 2024: does not distinguish between CIOG systems and Group/Service systems; has set the minimum level for risk acceptance as SES Band 1 or 1 Star; and does not refer to CSA or CSE roles.

Source: ANAO analysis of DSPF.

2.12 The DSPF also includes tables to outline the specific personnel appointed to the roles of Authorising Officer, Assessment Authority, Cyber Security Executive (CSE) and Cyber Security Advisor (CSA) for 14 Defence Services or Groups and five 'Special Portfolios'.[23] As noted in Table 2.1, these positions are the key decision-makers for system assessment and authorisation.

2.13 Until DSPF Control 23.1 was updated in May 2024, the following details were missing for the six years since the DSPF was established in 2018:

- the responsible CSE had not been defined for 13 Services or Groups;
- the responsible CSA had not been defined for 12 Services or Groups; and
- the responsible Authorising Officer, Assessment Authority, CSE, and CSA had not been defined for three special portfolios.

2.14 Further, the Groups and Services reflected in the DSPF had not been updated to reflect structural changes made in Defence since July 2020. For example:

- various groups are not included, such as the Associate Secretary Group, Australian Defence Force Headquarters, Defence Intelligence Group, Guided Weapons and Explosive Ordnance Group, and Naval Shipbuilding and Sustainment Group; and
- four Groups listed either no longer exist or have been renamed.[24]

23 The five special portfolios are: Australian Defence Simulation and Training Centre; Australian Signals Directorate; Australian Geospatial-Intelligence Organisation; Defence Intelligence Organisation; and Defence Industry Security Program.

24 The DSPF table refers to the: Chief Information Officer Group which transitioned to the Defence Digital Group in 2023; Estate and Infrastructure Group which transitioned to the Security and Estate Group in 2021; Chief Finance Officer Group which transitioned to the Defence Finance Group in 2018; and the Capability Development Group, which was replaced by the introduction of the Capability Acquisition and Sustainment Group in 2015.

2.15 Defence's September 2022 draft Cyber Security Enterprise Governance Framework, established to consolidate and describe the governance arrangements that support cyber security in Defence, noted that:

> The DSPF … is out of date with references to roles and responsibilities that are no longer relevant, to authorities and delegations that do not match the positions and there are several gaps or areas with TBC roles, responsibilities and expectations have not been defined. Some updates to the DSPF are planned however, more are required and the cadence for these updates needs to be more frequent to keep up with the evolving security landscape.

2.16 As a result of the May 2024 update, the DSPF Control 23.1 no longer includes a table of specific personnel appointed to key decision-making roles, but states that '[t]he list of the appointments for Groups and Services who can assess and authorise Defence ICT systems prior to operational use can be located on the Defence Intranet'. The DCIAB intranet page includes a list of 'functional appointments for Groups and Services across Defence' that was updated in April 2024. The updated list aligns with the current Defence organisational structure, and the Assessment Authority and Authorising Officer appointments are complete for all Groups and Services. The list of appointments does not include CSA or CSE roles.

Assessment and authorisation independence requirements

2.17 As outlined in Table 2.1, Security Assessors are required to maintain independence throughout the assessment process. Under the July 2020 DSPF Control 23.1, System Owners were required to maintain independence from the Authorising Officer.[25]

2.18 Defence advised the ANAO in February 2024 that Conflict of Interest and Statutory Declaration forms are completed for each contractor, and that it maintains a list of contractors against each Security Assessor to ensure they are not assigned assessment of a system to which a company in their employment chain has a stake.[26] Defence further advised that 'This process is not currently formalised within policy.'

2.19 Defence advised the ANAO in May 2024 that independence between the System Owner and Authorising Officer is maintained 'through checks performed by the Certification Consultant [Security Assessor] as part of commencing and completing the Security Assessment Report and development of the [Decision] Brief' and that this check 'is not currently formalised in [Assessment and Authorisation] process documentation'.

Delegating system authorisation

2.20 PSPF Policy 11 notes that 'An impartial (and in some cases independent) security assessment can be a valuable tool in authorisation decisions.' As outlined in Table 2.2, under the July 2020 DSPF Control 23.1, the CISO was the Authorising Officer, responsible for authorising high-risk Group/Service managed systems where a CSE has not been appointed. As outlined in Table 2.1, the Assistant Secretary of the ICT Security Branch, who fulfils the role of CISO, is also the Assessment (Certification) Authority, responsible for assessing all ICT systems except those within Air Force. Thus, under the July 2020 DSPF Control 23.1, for high-risk Group/Service managed systems where a CSE had not been appointed, the CISO could both assess and authorise those systems. For

25 This requirement was also in the July 2018 version of DSPF Control 23.1, but the requirement was removed when DSPF Control 23.1 was updated in May 2024.

26 The list provided by Defence includes details of 55 contractors and APS personnel.

significant-risk Group/Service managed systems where a CSA had not been appointed, the Authorising Officer was the ITSA, who reports directly to the CISO. The May 2024 updated DSPF Control 23.1 and associated list of appointments (see paragraph 2.16) no longer provides for the CISO or ITSA to fulfil Authorising Officer roles.

2.21 ANAO analysis of Defence's ICT authorisation management system data identified systems where the CISO was recorded as both the Assessment Authority and Authorising Officer. Of the systems which had an Authorising Officer recorded, 7 per cent had recorded the Authorising Officer as the 'Chief Technology Officer / Chief Information Security Officer'. For 18 per cent of those systems the CISO was also the Assessment (Certification) Authority.

2.22 Army, Navy and Air Force have each appointed CSAs and CSEs. Chief of Army Directive 02/20, issued in March 2020, states that, while the Director General Special Operations Modernisation is not a CSA, that position is responsible for authorising systems with significant risk.[27] The DSPF does not provide for the Authorising Officer role to be delegated to this position.[28] Army Standing Instruction (Protective Security) was signed by the Chief of Army in August 2022, and superseded Directive 02/20. The Standing Instruction appointed the CSA role to the Director General Land Operations.[29]

2.23 In response to an internal audit in May 2020 into *Certification and Accreditation of Defence ICT Networks*, which found that Defence's assessment and authorisation process lacked clarity and consistency, Defence advised that it would conduct an 'evaluation of current delegated Accreditation and Certification Authorities and determination of the appropriate approach to future delegation of Accreditation and Certification Authority'.[30] Defence advised the ANAO in March 2024 that amendments to delegations are being made as part of the transition to the Assessment and Authorisation Framework (see paragraphs 2.49–2.51).

Recommendation no. 1

2.24 The Department of Defence ensure that DSPF roles and requirements for system assessment and authorisation are complete, current, and regularly reviewed for alignment with the PSPF and Group/Service appointments.

Department of Defence response: *Agreed.*

2.25 *Defence will implement a continuous improvement function for the assessment and authorisation (A&A) approach as part of the newly established Cyber Security Policy hub. This function will be responsible for maintaining currency of all A&A delegations and authorities, as well as ensuring continued alignment and compliance with the PSPF and ISM.*

27 As at 12 August 2024, Defence's Chief of Army Directives intranet page still provided access to a July 2018 version of the directive and did not reflect that the July 2018 directive had been rescinded.

28 The DSPF identifies the Director Land Network Integration as the CSA.

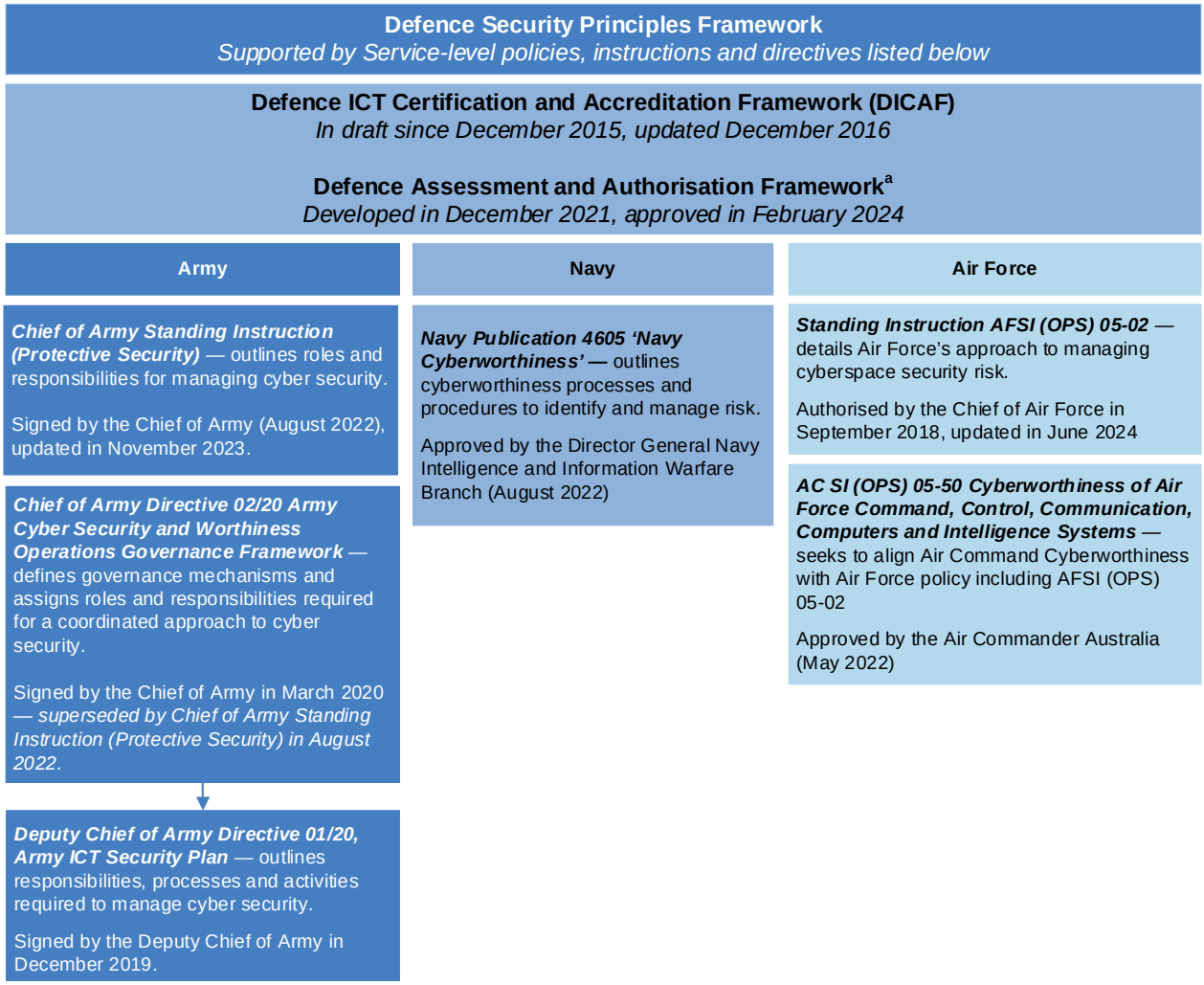
29 A separate Deputy Chief of Army Directive 01/20 *Army ICT Security Plan*, issued in December 2019 appointed the CSA role to the Director General Systems and Integration.

30 The May 2020 internal audit was conducted in response to a recommendation in a 2019 internal review for a Defence-level audit of authorisation processes. The 2019 review found that there was poor documentation of decision-making in the authorisation process, insufficient independent review and validation of information submitted by System Owners, and inconsistencies in the identification of Authorising Officers for ICT systems.

ADF service group policies

2.26 Army, Navy and Air Force have each issued policies, instructions or directives to support compliance with DSPF Principle 23 and Defence's assessment and authorisation process (discussed at paragraphs 2.53–2.73).[31] Figure 2.1 outlines the documentation issued by Army, Navy and Air Force to support DSPF Principle 23 as at July 2024.

Figure 2.1: Service-level documents supporting the DSPF



Note a: Defence advised the ANAO in August 2024 that the Assessment and Authorisation Framework 'was developed to replace the DICAF'.

Note: Where a document hierarchy has been established in Service issued documentation, this is reflected by arrows in Figure 2.1. The remaining documents are ordered by the seniority of the approving officer.

Source: ANAO analysis of Defence documentation.

2.27 In December 2019, the Deputy Chief of Army issued Directive 01/20 *Army ICT Security Plan* to 'provide clear direction on the responsibilities, processes and activities required to effectively manage the Cyber Security and Worthiness of Army's in-service ICT and information assets.' In this context, the directive:

31 See Figure 1.2 for Defence's administrative policy framework which outlines the hierarchy of Defence documents.

- states that 'all Army ICT systems must be accredited prior to processing, storing or communicating unofficial, official, sensitive or classified Defence information'; and
- outlines System Owner responsibilities for monitoring the expiry of system authorisations and seeking re-authorisation, as well as the requirements for system security documentation.

2.28 For 'Some Distribution Limitation Marker (DLM) or FOUO [For Official Use Only] systems' the Chief of Army directive provides for a 'streamlined security assessment' and approval process 'in lieu of a formal certification and accreditation.'

2.29 Defence advised the ANAO in April 2024 that this streamlined process was 'a reference to an old and obsolete … whitelisting process and that all Defence (Army) systems are to go through the normal accreditation process'. Defence also advised that:

> the updated version of the Army ICT Security Plan (currently awaiting delegate approval) states "IAW [in accordance with] DSFP Principle 23, all Army ICT … systems must be accredited prior to processing, storing or communicating official or classified Defence information".

2.30 As noted at paragraph 2.27, this requirement was set out in the 2019 Deputy Chief of Army directive. Defence advised the ANAO in June 2024 that the Army ICT Security Plan was 'in the final stages of review prior to release'.

2.31 In August 2022, Defence released a Navy 'Cyberworthiness' policy, approved by the Director General of Navy Intelligence and Information Warfare to 'significantly reduce cyberworthiness risks to all Navy owned ICT … materiel and support systems.'[32] The policy notes that the DSPF is the 'authoritative source for managing security risks and their associated controls', and outlines the ISM six-step process for system assessment.

2.32 Defence acknowledges in the cyberworthiness policy that some inconsistency exists between the policy and the DSPF — namely, that Navy's system for rating risks does not align with the DSPF's risk evaluation matrix.[33] The policy also states that the Chief of Navy is the System Owner for all Navy systems and the Authorising Officer for systems with a risk rating of 'Extreme'. This means that for systems with an 'Extreme' risk, the Chief of Navy is both the System Owner and the Authorising Officer — a situation that does not align with the DSPF. As outlined in Table 2.1, the July 2020 DSPF requires the System Owner to be independent of the Authorising Officer.

2.33 Air Force instruction AFSI (OPS) 05-02, issued in September 2018, details Air Force's approach to managing cyberspace security risk. The instruction establishes the Commanding Officer of 462 Squadron (462SQN) as the 'Certification Authority' for Air Force and states that 'Air Force information systems owners may use other DSPF authorised Certification Authorities if 462SQN is unable to support (due to either lack of capacity or specialist skill requirements) or where a more suitable option exists'.

2.34 The instruction requires that Air Force information systems are assessed and authorised in accordance with the ISM and DSPF. The instruction also states that:

32 The policy defines cyberworthiness as 'a measure of a capability's suitability to operate in its intended environment.'

33 While Navy uses a five-point risk rating scale like the DSPF, the risk categories are different. Army also uses a five-point rating scale which does not align with the risk ratings outlined in the DSPF. Defence advised the ANAO in June 2024 that Air Force risk assessments are consistent with the DSPF scale.

> Where a system is to be force assigned[34] without or with partial certification, risks and limitations are to … be recorded as part of the certification.

2.35 This statement is not aligned with the DSPF requirement that all Defence ICT be authorised prior to processing, storing or communicating official information. This statement is also not in accordance with Chief of Joint Capabilities Directive 07-20 *ADF Cyberworthiness Governance Framework,* issued in December 2020, which states that Capability Managers 'are to ensure that only certified and accredited mission systems are force assigned to operations, and that this status is verified during pre-deployment'. The directive outlines that the ADF Cyberworthiness Governance Framework is for 'implementation across the Services to ensure cyberworthiness efforts are streamlined, consistent and effective.'

2.36 A further Air Force instruction, AC SI(OPS) 05-50 *Cyberworthiness of Air Force Command, Control, Communication, Computers and Intelligence Systems,* issued in May 2022, also outlines assessment and authorisation requirements. The instruction notes that:

> a Provisional ICT Accreditation (PICTA) is awarded where the Accreditation Authority has requested further controls and/or risk mitigation activities to be undertaken during the provisional accreditation period …
>
> A PICTA achieves efficiencies through reduced rework of C&A [Certification and Accreditation] activities. Ref D [AFSI (OPS) 05-02 – Cyberworthiness, Certification and Accreditation] identifies that a PICTA may be upgraded to an ICTA without undertaking a full re-certification activity.

2.37 AFSI (OPS) 05-02 does not address the issuing of provisional authorisations and the DSPF does not provide for provisionally authorised systems to be re-authorised without undertaking a full re-assessment activity.

2.38 The Deputy Chief of Air Force approved an updated version of AFSI (OPS) 05-02 in June 2024. The 2024 instruction does not refer to provisional authorisation and requires all Air Force systems to be authorised prior to operation. The 2024 instruction provides for moderate and low risk systems to be authorised by personnel below Senior Executive Service (SES) 1 or 1 Star officer level. This does not accord with the updated May 2024 DSPF Control 23.1, which requires SES 1 or 1 Star authorisation of these systems.

Defence ICT Certification and Accreditation Framework

2.39 The Defence ICT Certification and Accreditation Framework (DICAF) was developed by the ICT Security Branch (now DCIAB) to 'ensure that Certification and Accreditation activities are conducted in a repeatable and consistent manner across [Defence]' and applies to all Defence ICT systems that process, store or communicate official, sensitive or classified information.

2.40 The DICAF has been in draft since December 2015 and was last updated in December 2016.

2.41 The DICAF provides a high-level overview of Defence's assessment and authorisation requirements. It outlines which systems are subject to the assessment and authorisation requirements and defines the roles and responsibilities of personnel involved in the system authorisation process. A section outlining the detailed process for system assessment and

34 Force assignment is the assigning of forces to a commander under a state of command, an operational authority, an administrative authority or support arrangement for the purpose of carrying out a specified mission or task.

authorisation was to be developed and included with a supporting annex to the DICAF. At July 2024, the process section and the supporting annex had not been developed.

2.42 A draft February 2017 ICT Security report[35] provided a progress update on the development of the DICAF and stated that:

> Progress is being made to update the draft DICAF based on feedback received from the DICAF Working Group and other stakeholders. It is anticipated that the DICAF will be in releasable format by mid-2017.

2.43 The 2018–19 DSPF Control Owner report for DSPF Control 23.1[36] provided an update on the DICAF in July 2019, stating that:

> ICTSB [now DCIAB] is currently reviewing the extant Cyberspace Security Governance Framework[37] with the intention for the new Framework to become a charter to improve stakeholder investment. It is intended that it will absorb the Defence ICT Certification and Accreditation Framework (DICAF) to align cybersecurity governance roles and responsibilities.

2.44 This statement was repeated in the 2019–20 control owner report in July 2020.

2.45 Defence's Cyberspace Security Governance Framework (CSGF) was last reviewed in November 2016 (as at July 2024). The CSGF states that the DICAF forms part of the 'related documents and legislation' for the CSGF. Defence advised the ANAO in March 2024 that:

> The Cyberspace Security and Governance Framework (CSGF) is a legacy left over from the original establishment of, and appointments … of the Defence CISO and ITSA in 2015-16 … The decision to delay its revision (as specified in the Control Owners Reports 2018-2019 & 2019-20) was largely because events had overtaken matters with responsibilities of the Cyber Security Governance Board (CSGB) moving across to the enterprise governance committee structures (such as the Defence Security Committee), [which] had achieved improvements to the oversight and control of cyber security related matters. This along with the anticipated changes in cyber security governance expected through the design and delivery of the Defence Cyber Security Strategy and the changes scheduled through [the ICT Security Program] (including the A&A [Authorisation and Assessment] framework) became the primary focus of effort.[38]

2.46 Defence's May 2020 internal audit into *Certification and Accreditation of Defence ICT Networks* identified 'risks within the existing certification and accreditation process for ICT networks and systems which are not being controlled effectively by the Department.' The report found that there were inconsistencies in the authorisation processes being applied across Defence, and that

35 Defence advised the ANAO in June 2024 that it was unable to locate the final version of this report. There was no evidence to identify who prepared the report and who it was provided to.

36 Control Owners reports and reporting requirements are discussed at paragraphs 3.52–3.65.

37 The Cyberspace Security and Governance Framework was developed to 'identify and establish the mechanisms and information sharing necessary to ensure Cyber Security is coordinated across Defence.' The CSGF records an 'initial issue' date of January 2016 for Version 1.0 of the document. Version 0.6 of the document is noted as a 'final draft' and is dated October 2016.

38 Defence's Assessment and Authorisation Framework is discussed at paragraphs 2.49–2.51. The ICT Security Program is discussed at paragraph 3.12.

the DICAF did not provide sufficient guidance for identifying what systems require authorisation and ensuring a risk-based approach is applied during system assessments.[39]

2.47 The internal audit recommended that 'CIOG should re-assess the design of its current Certification and Accreditation Framework, including (as relevant) the policy setting and detailed processes and procedures adopted for the certification and accreditation of ICT networks and systems.'[40]

2.48 In February 2021, DCIAB's Directorate of Integrated Risk Management (now the Directorate of Cyber Security Assessments and Authorisation) held a meeting to discuss the development of the DICAF in response to the internal audit findings. The meeting presentation noted that:

> There is no authoritative source that defines the "framework". Previous draft iterations of the Defence ICT Certification and Accreditation Framework (DICAF) did not provide adequate coverage in terms of end to end processes.

2.49 In December 2021, Defence's Head of ICT Operations (HICTO)[41] signed a minute recommending the internal audit recommendation be closed, and outlining action taken to address the findings, including the development of 'a modernised Certification and Accreditation Framework, known as the Defence Authorisation and Assessment Framework.'

2.50 The framework remained in draft until a final version was approved by the CISO in February 2024 and released in May 2024.

2.51 The framework: outlines roles and responsibilities for assessment and authorisation; defines the systems to which the framework applies; and outlines Defence's process requirements against each step of the ISM's six-step process. The framework does not mandate the inspection and validation of control implementation as part of the assessment and authorisation process for all systems. This is not consistent with Step 4 of the six-step process (see Figure 1.1) which requires entities to validate security controls to determine they have been correctly implemented and are operating as intended.

Has Defence developed fit-for-purpose guidance to support the implementation of its framework?

Defence does not have an up-to-date set of consolidated guidance to support the implementation of its framework in a consistent manner across the organisation. Defence's assessment and authorisation process guidance is internally inconsistent and a number of supporting templates have not been finalised or are outdated. Separate instructions, directives

39 Internal Audit allocated these findings a risk rating of 'High', the second highest severity rating on its five-point rating scale. The definition of 'High' is 'A weakness highly likely to significantly compromise the internal control framework of the business area concerned. High potential for a major adverse effect on the business operations, reputation, staff well-being or financial loss. Requires prompt short term remedial action by Executive Management within the next 3 to 6 months'.

40 Defence agreed to the recommendation and proposed to address it through: implementation of an 'ICT Security Program' by August 2021 (see paragraph 3.12); the development of an inventory of all Defence ICT systems by December 2021 (see paragraphs 3.7–3.11); and a review of staffing levels and development of a supporting business case for staffing and resources by September 2020 (see paragraph 3.22).

41 Prior to a restructure in December 2023 (see footnote 19) the CISO reported to the HICTO.

and policies exist for the Army, Navy and Air Force, which include some requirements that are inconsistent with Defence's assessment and authorisation process, the DSPF and PSPF.

2.52 In September 2021, an assessment and authorisation process was published on the Defence intranet. Documentation developed and issued by Army, Navy and Air Force (see paragraphs 2.26–2.38) refers to the assessment and authorisation process, and stipulates additional requirements and templates, discussed further in the context of the Defence process below.[42]

Defence's assessment and authorisation process

2.53 Defence's assessment and authorisation intranet process sets out four steps: 'lodge certification and accreditation request'; 'conduct certification assessment'; 'review certification assessment'; and 'finalise certification and accreditation'. A responsibility assignment matrix is documented at each step, outlining responsibilities for key tasks and links to the ISM and DSPF.

2.54 While the intranet process was published on Defence's intranet after PSPF Policy 11 was amended in August 2020, the process does not reflect the updated language in PSPF Policy 11.[43] The process also does not fully reflect the ISM's six-step process for system assessment and authorisation.[44] At July 2024, the assessment and authorisation process was no longer accessible on Defence's intranet. Defence advised the ANAO in July 2024 that this was due to the intranet page no longer being supported internally and that the content would be made accessible 'as resourcing allows'.

2.55 A summary of Defence's assessment and authorisation process is shown in Figure 2.2.

Lodge certification and accreditation request

2.56 Requests for the assessment and authorisation of ICT systems are lodged by System Owners or their delegates through Defence's ICT intranet job portal. The portal requires System Owners to provide key information, including the required operating date for the system, urgency of the request and system classification level. The request is then assessed by a 'Security Analyst' to ensure that sufficient information has been provided and to confirm the priority of the request.

42 While Air Force documentation provides links to the Defence assessment and authorisation process, it also establishes the Commanding Officer of 462 Squadron (462SQN) as the Certification Authority for Air Force systems (see paragraph 2.33). Air Force has also established a separate assessment and authorisation process. Defence advised the ANAO in April 2024 that Air Force's 'extensive use of aviation technology and foreign military sales' requires specialised knowledge and that Air Force has 'maintained its subject matter expertise in the Cyber Security Space'. In March 2024, 462SQN transitioned to Cyber Command in the Joint Capabilities Group (the same group as DCIAB).

43 As noted at paragraph 1.10, prior to August 2020, PSPF Policy 11 used the terms 'certification' and 'accreditation.' Since August 2020, PSPF Policy 11 refers to 'assessment' and 'authorisation.' This report uses the terms 'assessment' and 'authorisation' unless quoting from Defence documents.

44 Defence's intranet process does not require the documentation of control implementation assessment (Step 3) and does not discuss ongoing monitoring of ICT systems after authorisation (Step 6).

2.57 The System Owner is also required to enter system information into Defence's ICT authorisation management system[45], including the assessed Business Impact Level[46], and system threats and risks. The System Owner is also required to provide a System Security Plan (SSP) and System Risk Score document.

2.58 Defence's System Risk Score document enables DCIAB to assess the overall system risk and allocate a risk score, based on the System Owner's Business Impact Level assessment, system characteristics and potential security management controls. The System Risk Score template is a mandatory document under the assessment and authorisation process. As at July 2024, the October 2013 template had not been updated to reflect Essential Eight requirements.[47] The document does not have a stipulated period for review.[48]

2.59 Defence's SSP template outlines the information on the system to be authorised, description of system threats and safeguards, compliance with Essential Eight requirements, and processes for detecting and responding to cyber security incidents. The SSP requires executive sign-off and approval prior to being submitted, however neither the assessment and authorisation process nor the linked SSP template identifies the appropriate authority for sign-off.

2.60 Defence advised the ANAO in March 2024 that:

> Under the DSPF … System Owners are responsible for developing relevant security artefacts for their systems. If the sign-off/approval requirement is not well understood by the System Owner and/or team, the Certification Consultant will clarify this. However, there is currently no formal or specific guidance advising that the System Owner is the one who signs off on the SSP. This potential ambiguity is being resolved in the latest A&A [Assessment and Authorisation] framework release.

2.61 The Assessment and Authorisation Framework, released in May 2024, did not include any requirements in relation to a SSP sign-off. In June 2024, Defence provided the ANAO with an updated SSP template from March 2024 (which was available on the Cyber Security Assessment and Authorisation intranet page).[49] Guidance within the template states that the SSP should be approved by the System Owner.

45 Air Force's separate process does not outline a requirement for system information to be entered into Defence's ICT authorisation management system.

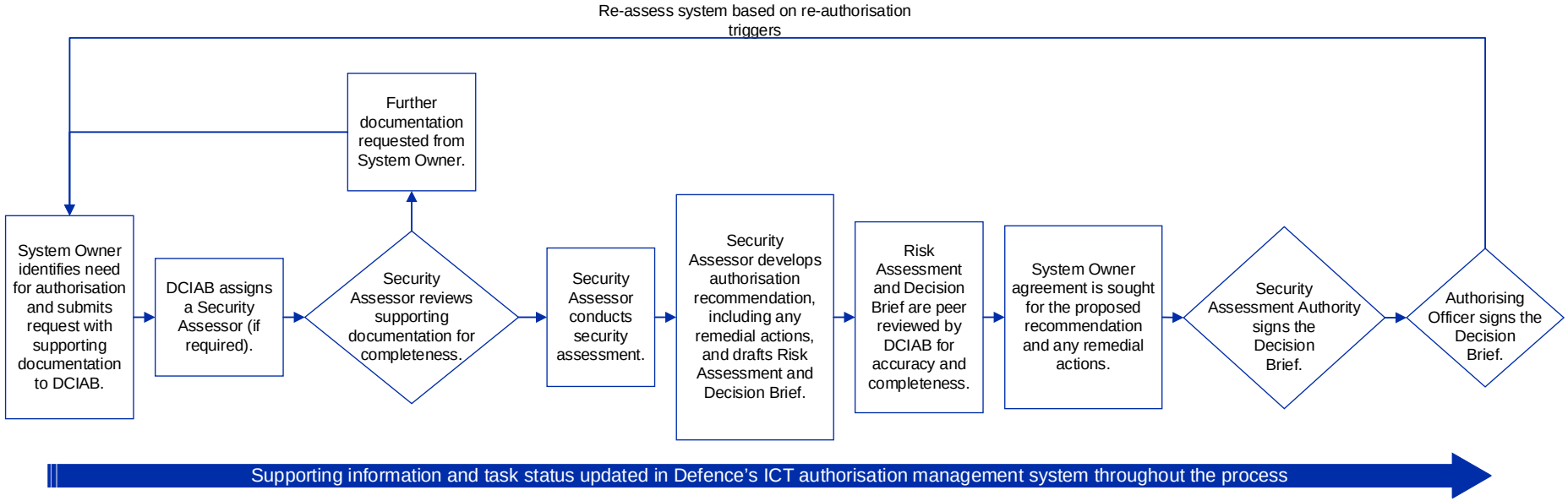
46 Business Impact Level assessments consider the potential damage arising from the loss or compromise of confidentiality, integrity or availability of Australian Government resources. Business Impact Level assessments are required under DSPF Principle 25 *Information Systems Business Impact Levels and Aggregation* which stipulates that 'Defence and Defence Industry information systems that store, process or communicate Official Information are assigned [Business Impact Levels]'.

47 The template refers to the 'Essential – Top 4 Strategies', which is a subset of the Essential Eight strategies. As noted at paragraph 1.7, PSPF Policy 10 was amended in February 2022 to mandate all eight strategies.

48 Defence's intranet guidance as at February 2024 advised that the System Risk Score document had been replaced from 1 January 2023 with a SSP Essential Eight Annex. As at 13 August 2024, Defence's assessment and authorisation intranet process, and supporting templates, had not been updated to reflect this requirement.

49 Defence advised the ANAO in August 2024 that it did not retain a record of the date on which the SSP template was made available on the intranet.

Figure 2.2: Defence assessment and authorisation process, as at May 2024



Source: ANAO analysis of Defence records.

2.62 Defence's assessment and authorisation process lists other documentation that 'may be required depending on the nature and complexity of the system' including: the SSP Essential Eight Annex[50]; Security Risk Management Plan (SRMP)[51]; Defence Logging and Monitoring Guide; Defence Continuous Monitoring Guide; Standard Operating Procedures (SOPs)[52]; and Incident Response Plan (IRP).[53] As at June 2024, the templates for the Defence Logging and Monitoring Guide, Defence Continuous Monitoring Guide, and IRP were all listed as 'pending' in the process. Defence advised the ANAO in June 2024 that these templates remain under development and are expected to be finalised by August 2024.

2.63 Step 5 of the ISM six-step assessment and authorisation process states that:

> Before a system can be granted authorisation to operate, sufficient information should be provided to the authorising officer in order for them to make an informed risk-based decision as to whether the security risks associated with its operation are acceptable or not. This information should take the form of an authorisation package that includes the system's system security plan, cyber security incident response plan, continuous monitoring plan, security assessment report, and plan of action and milestones.

2.64 Defence advised the ANAO in February 2024 that there is no formal guidance to assist in making the judgement as to whether these additional documents are required as part of the assessment and authorisation process, and that 'the need for additional documents … will be identified during the certification process and communicated to system delegates'.[54]

2.65 Following the submission of information and documentation by the System Owner, a Security Assessor (Certification Consultant) and Peer Reviewer are assigned to the task through Defence's ICT authorisation management system.

50 The SSP Essential Eight Annex allows users to assess system maturity against Essential Eight requirements, including assessing the implementation of relevant Essential Eight controls outlined in the ISM.

51 In the SRMP template, for each system risk identified, the System Owner completes a Risk Assessment Form which includes a description of the threat, controls, treatment options, and residual risk. The Navy Cyberworthiness Policy, Army ICT Security Plan Directive (see paragraphs 2.26–2.32), and Air Force assessment and authorisation process all require completion of the SRMP.

52 The Air Force authorisation process includes assessing the content of SOPs as a standard part of the process. Army guidance states that 'SOPs are required as part of the system security documentation suite'.

53 DSPF Control 24.1 *Information Systems Security Incident Management* requires that 'Systems are to be covered by an Incident Response Plan (IRP). The size and complexity of the system determines whether an individual system requires its own IRP … IRPs comprise one element of the documentation suite required for system certification and accreditation'.

Further, the Navy Cyberworthiness Policy (see paragraphs 2.31–2.32) states that an IRP is required, and Army's assessment and authorisation intranet page states that an Army Cyber Security IRP is 'provided as part of supporting material for the Certification and Accreditation/Authorisation evaluation' and provides a link to an Army IRP template. The Air Force assessment process includes assessing the content of the IRP as a standard part of the process.

54 Defence further advised that 'documents such as a Logging and Monitoring Plan, Continuous Monitoring Plan and Incident Response Plan will be required if a system is not hosted on a platform already covered by such documents. Standard Operating Procedures will be required if there are risk mitigations that require procedural actions to effect, such as applying manual patches, manual file transfer procedures, and user access provisioning.'

Conduct certification assessment

2.66 The Security Assessor reviews the security documentation provided to ensure that documentation is complete and engages with the System Owner if further information is required.[55] Once the Security Assessor has sufficient information, they conduct a 'Stage 1 Assessment' which includes: a detailed analysis of the system design to assess risks; a determination as to whether appropriate security controls have been implemented; and a review of all relevant controls specified in the ISM and DSPF.

2.67 The Security Assessor also determines whether a cyber assessment is required, based on risk appetite, security requirements, and threat data.[56] A 'Stage 2 assessment' may also be conducted if the system is a high profile, high risk, or highly complex system and involves cross-checking system inspection findings against documentation to verify the implementation of security controls.[57]

2.68 Following the assessment, the Security Assessor prepares a Risk Assessment and Decision Brief outlining the security posture of the system, the assessed residual risk, and any suggested remediation actions. If further actions are required, a Remediation Plan may be developed by the Security Assessor and sent to the System Owner.

Review certification assessment

2.69 The Risk Assessment and Decision Brief are reviewed by a peer reviewer. The peer reviewer is a Security Assessor within DCIAB's Certification Management team[58] who conducts a quality assurance check of the Risk Assessment and Decision Brief to assess accuracy and completeness, and determine that the correct approvers have been identified. The report is also reviewed by the System Owner, and any caveats or recommendations, as well as the proposed authorisation outcome are agreed on.

2.70 Once the System Owner has agreed to the Risk Assessment and Decision Brief, the Risk Assessment is signed by the Security Assessor and submitted to the Assistant Director or Director of DCIAB's Cyber Security Assessments and Authorisation (CSAA) Directorate for final review and sign-off before progressing to the Assessment (or Certification) Authority.

55 A 'System Overview Document' (SOD) is listed in the 'Conduct certification assessment' step of Defence's assessment and authorisation process as one of the documents assessed by the Security Assessor. The SOD is not referred to elsewhere in the other steps of Defence's process, and does not have a linked template. Defence intranet guidance states that 'An assessment by Defence Cyber and Information Assurance Branch is based on the information provided within the System Overview Document.' The intranet guidance also states that, from 1 January 2023 the SOD was no longer in use and had been incorporated into the SSP.

56 Cyber assessments take the form of vulnerability assessments and penetration testing.

57 The Assessment and Authorisation Framework (see paragraphs 2.49–2.51) outlines that a Stage 1 assessment involves a 'desktop review of system documentation and assessment of the design of cyber security controls', while a Stage 2 Assessment 'involves validation and inspection of control implementation and operation'.
The ISM six-step process (see Figure 1.1) states that security controls for each ICT system are to be assessed 'to determine whether they have been correctly implemented and are operating as intended.'

58 Certification Management is a team within DCIAB's Cyber Security Assessments and Authorisation (CSAA) Directorate, responsible for assigning Security Assessors, determining assessment priorities, and conducting management reviews of Risk Assessments.

Finalise certification and accreditation

2.71 The Risk Assessment and Decision Brief then proceed to the Assessment Authority (which is the CISO for all Defence systems except for Air Force) for approval. The Decision Brief is supported by the CSAA Directorate approved Risk Assessment, which is included as an attachment to the brief. Once approved by the Assessment Authority, the assessment and brief are then sent to the Authorising Officer for further approval, noting acceptance of the residual risk in operating the system.[59] The System Owner is required to be advised of any caveats on the authorisation, and documentation is to be filed to Defence's records management system, Objective.

Recommendation no. 2

2.72 The Department of Defence conducts a review of, and updates, its assessment and authorisation process documentation to ensure:

(a) alignment with current DSPF and PSPF requirements;

(b) consistency across all internal guidance documents, including those developed by the ADF Services; and

(c) that any internal inconsistencies within individual guidance documents are eliminated.

Department of Defence response: *Agreed.*

2.73 *Defence is formalising an A&A [Assessment and Authorisation] Improvement Program to build on and consolidate the current set of A&A initiatives underway. Defence will undertake a comprehensive integrated review of the A&A approach, policies, processes and documentation.*

Has Defence developed fit-for-purpose training and other support for personnel responsible for implementing its framework?

Defence has not established training to ensure that Security Assessors remain up-to-date on evolving cyber security requirements, instead relying on peer review and Assessment Authority review to mitigate any 'deficiencies in knowledge'. Deficiencies were identified in Defence's implementation of the peer review process and Defence does not undertake assurance activities to monitor the extent to which training is completed. The absence of a formalised training approach to support the implementation of DSPF requirements for the assessment and authorisation of ICT systems creates a risk that systems are not being authorised as intended. Defence data on ICT system authorisations shows that 47 per cent of its systems have a status of either 'Expired' or 'No accreditation', indicating that System Owner obligations in respect to obtaining and maintaining the authorisation of their systems are not being met.

59 Guidance in the Security Risk Management Plan (SRMP) template (see footnote 51) states that 'Extreme' risks are 'too high and must be immediately managed by mitigation strategies.' The template states that 'High' risks are 'probably too high and should be promptly managed by mitigation strategies.' Supporting guidance for Air Force recommends that systems with extreme and high-risk ratings are only accredited for one and two years respectively.

2.74 Specific training requirements in relation to ICT system assessment and authorisation have not been established in the DSPF. Prior to the DSPF being introduced in July 2018, the Defence Security Manual (DSM) required that Security Assessment Authorities and Authorising Officers, as well as external service providers engaged to perform assessment and authorisation activities, successfully complete an approved course of training.[60]

2.75 Specific system authorisation training requirements have been established by Army. High-level training requirements have also been established by Navy.[61] Deputy Chief of Army Directive 01/20 *Army ICT Security Plan* (see paragraphs 2.27–2.30) requires that Information Technology Security Managers (ITSMs) and Information Technology Security Officers (ITSOs)[62] complete courses including: cyber security awareness[63]; ICT certification and accreditation; and an ITSO/ITSM course.

Information Technology Security Officer/Manager course

2.76 The ITSO/ITSM course includes assessment and authorisation content such as: roles and responsibilities throughout the assessment and authorisation process; Army's assurance arrangements, which include assessing the authorisation status of systems (see paragraphs 3.33–3.34); and stipulating that changes to an ICT system may require re-authorisation.[64]

2.77 Defence advised the ANAO in February 2024 that:

> an updated [Army] ICT Security Plan is currently awaiting DCA [Deputy Chief of Army] approval. A substantial change in the updated plan is the decoupling of system owner responsibilities from a unit's cyber security management responsibilities. It was agreed that a unit cannot be a system owner … and as such generally does not get involved in C&A [Certification and Accreditation] activities. Therefore, the requirement to undertake targeted C&A training has been removed from the ITSO duty statement. However, ITSOs are still required to be aware of C&A at a high level, which is contained within the updated Army ITSO Course.[65]

60 Defence advised the ANAO in June 2024 that this training was a course for Information Technology Security Managers (ITSMs) and Information Technology Security Officers (ITSOs) similar to the ITSM/ITSO course provided by Army (discussed at paragraphs 2.76–2.77). Defence further advised that the completion of the course 'was both tested and recorded, however, the course/system is now non-operational, therefore Defence is unable to verify if records were maintained of who successfully completed the course.'

61 The Navy Cyberworthiness Policy requires that all personnel 'involved in any aspect of the Navy owned ICT and OT maritime materiel and support system cyberworthiness and cyberspace security responsibilities are to receive training commensurate to their expected roles, to ensure a positive effect on cyberworthiness and cyberspace security.'

62 ITSOs are unit-level officers responsible for implementing and monitoring requirements outlined in the Army ICT Security Plan for systems for which they are responsible, under the guidance of the ITSM.

63 Defence advised the ANAO in January 2024 that the cyber security awareness course has been incorporated into Defence's Annual Security Awareness course. The DSPF requires all Defence personnel and contractors to complete Annual Security Awareness training. The references to system authorisation in this training related to informing personnel of the requirement to only use authorised systems to access Official information.

64 The course states that 'If the change is determined by the system owner as minor (low risk) no further action is required until the system is routinely re-accredited'. The DSPF states that ICT systems are to be re-authorised when 'changes to the certified system architecture occur'.

65 Defence advised the ANAO in June 2024 that the updated Army ICT Security Plan 'is in the final stages of review'.

ICT Certification and Accreditation Campus course

2.78 Between 2010 and 2020, Defence offered an ICT Certification and Accreditation Course through one of its online e-learning and training platforms, Campus. In May 2020, DCIAB advised Defence's Security and Vetting Service that:

> the ICT Certification and Accreditation Course is no longer required on Campus as the content is out of date and now obsolete.
>
> Comprehensive information regarding the ICT Certification and Accreditation process is now available within ICT Security Integrated Risk Management Portal.[66]

2.79 Defence advised the ANAO in February 2024 that it did not retain the course content and therefore could not provide it. Defence was unable to provide data on course completion.

ICT Certification and Accreditation Roadshow

2.80 DCIAB has developed an ICT assessment and authorisation presentation which outlines the assessment and authorisation process, responsibilities of System Owners, triggers for re-authorisation, and the use of contracted assessors and associated conflicts of interest responsibilities.[67]

2.81 The presentation outlines that System Owners have an obligation to request an emanation threat assessment from the Australia Signals Directorate (ASD). Emanation Security relates to the protection of signals, which, if intercepted and analysed, could disclose classified information. The slides further note that '[w]hether the assessment is required or not is up to ASD to make that determination. Regardless, the system owner is obligated to request one prior to submitting their system for assessment. This should be done whilst completing the security documentation suite so it can be captured and articulated within the documents for the assessor'. Neither the DSPF nor Defence's assessment and authorisation process outline this requirement.[68]

2.82 Defence advised the ANAO in June 2024 that '[n]o records are available of when and to whom this roadshow presentation was delivered.'

ICT authorisation management system training

2.83 In 2019, DCIAB developed training courses for System Owners, Security Assessors and Authorising Officers using Defence's ICT authorisation management system. The training includes

66 As at July 2024, the ICT Security Integrated Risk Management Portal directed users to the Cyber Security Assessment and Authorisation (CSAA) intranet page, which included information on Defence's assessment and authorisation process.

67 The presentation is undated. Defence advised the ANAO in June 2024 that the presentation was developed in 'approximately August 2023'.

68 Emanation Security requirements are also not stipulated in the Army ICT Security Plan directive or Air Force instructions AFSI (OPS) 05-02 or AC SI(OPS) 05-50. Navy's Cyberworthiness policy states that 'for many Navy owned ICT … systems, the system will require both cyberworthiness and EMSEC certification and accreditation before use.'

process-oriented guidance for completing Business Impact Level assessments, completing key fields, uploading supporting documentation, and reviewing authorisation approvals or rejections.[69]

2.84 In weekly DCIAB reporting to the CISO (see paragraph 3.66) between January 2023 and June 2024, one instance was identified where completion of these courses was included in the reporting.

Security Assessor training

2.85 DSPF Control 23.1 states that a Security Assessor (Certification Consultant) must be 'suitably qualified' and is responsible for:

- providing advice and guidance to the System Owner on the assessment process; and
- providing advice and guidance on mitigation strategies and controls to reduce risk within an acceptable risk tolerance throughout all phases of system development.

2.86 The Cyber Security Assessment and Authorisation (CSAA) Directorate within DCIAB has developed a 'New Starter Information Pack' which includes an induction checklist for new staff, including familiarisation with Defence's ICT authorisation management system and supporting SOPs, the completion of mandatory training[70], links relating to the assessment and authorisation process, and an outline of the process for generating a Risk Assessment. The information pack's contents page also includes a reference to 'Annex B – Certification and Accreditation Process', however the annex is not present in the document. The new starter pack is dated August 2021, but formal approval has not been recorded in the document. Defence does not record or report on the completion of training for Security Assessors.

2.87 Since its release in 2009, the ISM has been regularly updated. Since December 2021, the ISM has been updated quarterly, including changes to ISM controls. Defence does not have a structured process in place to ensure that Security Assessors are aware of changes to ISM control requirements. Defence advised the ANAO in February 2024 that the System Security Plan Essential Eight Annex is 'routinely updated to reflect changes to ISM controls'[71] and that:

> Any deficiencies in knowledge that result in inadequate risk identification and control coverage is identified within the peer review process, and failing that, at Certification Authority review.[72]

2.88 The absence of a formalised training approach to support the effective implementation of DSPF requirements for the assessment and authorisation of ICT systems increases the risk that systems are not being authorised as intended. Defence data on the authorisation status of ICT systems (discussed at paragraphs 3.15–3.26) shows that 47 per cent of systems recorded in Defence's ICT authorisation management system have a status of either 'Expired' or 'No accreditation'. A September 2019 Air Force brief (see paragraph 3.44) identified that there was a lack of awareness of authorisation responsibilities, and Defence advised the ANAO in June 2024 that

69 The training was originally offered through Campus. Defence advised the ANAO in February 2024 that the training was removed from Campus as it 'contained Adobe flash content which was non-compliant with ASD Essential Eight Maturity Model', and that it 'is now done internally as part of the induction process for new starters who require access to the system'.

70 The mandatory Campus courses are: Fraud and Integrity Awareness; Security Awareness; Work Health and Safety; Workplace Behaviours; and Objective Course.

71 The Essential Eight Annex is discussed at footnote 50. The Essential Eight Annex linked in Defence's assessment and authorisation process reflects controls from the December 2022 ISM.

72 As outlined at paragraphs 3.83–3.85, deficiencies were identified in Defence's peer review process.

further improvements were required to assist System Owners in meeting their authorisation obligations (see paragraph 3.31).

Recommendation no. 3

2.89 The Department of Defence:

(a) implements improved training and awareness raising activities to ensure that key personnel involved in the assessment and authorisation process are aware of their obligations under the PSPF and DSPF, and remain up-to-date with evolving cyber security requirements; and

(b) implements a framework to monitor and report on the completion of training and awareness raising activities.

Department of Defence response: *Agreed.*

2.90 *A key line of effort in the A&A [Assessment and Authorisation] Improvement Program will be the design, development and implementation of A&A related training and awareness activities.*

Defence Cyber Security Strategy Action Plan

2.91 As discussed at paragraph 1.4, the Defence Cyber Security Strategy noted that one of Defence's most critical risks is cyber security. One objective of Defence's Cyber Security Strategy is to 'build awareness of cyber security threats and individual accountabilities, and uplift cyber security capability across the Defence workforce'.

2.92 To address this objective, Defence stated in its Cyber Security Strategy Action Plan, that 'An enterprise-wide cyber security training program will be established to deliver uplift across the enterprise' including:

- additional tiered training programs to address differing requirements based on position, and access to classified information and critical capabilities;
- development programs for all personnel involved in the design, management and security of Defence's cyber terrain; and
- training programs for senior executives to improve their understanding of, and ability to manage, cyber security risks.

2.93 Defence advised the ANAO in May 2024 that 'the training program under development within the Cyber Security Strategy Action Plan does not cover specific training for ICT Security Assessment and Authorisation'.

3. Implementation of arrangements for the security authorisation of Defence's ICT systems

Areas examined

This chapter examines whether the Department of Defence (Defence) has implemented arrangements for the security authorisation of its ICT systems.

Conclusion

Defence has partly implemented arrangements for the security authorisation of its ICT systems. Defence's data on its system assessments and authorisations is incomplete and indicates that System Owner obligations to obtain and maintain authorisation of their systems are not being fulfilled.

There were deficiencies in relation to Defence's monitoring and reporting arrangements, including non-compliance with DSPF reporting requirements. Key information on the authorisation status of Defence's systems was omitted from Defence's reporting, including not addressing a request from the Minister for Defence to include metrics in reporting on unapproved ICT systems within Defence. Defence's internal and external reporting on its assessments indicated a more optimistic outlook than was otherwise reflected in other internal Defence documentation. Across the ICT systems examined in case studies, deficiencies included: the absence of key data and mandatory security documentation; no evidence of assessment of control implementation; and deficiencies in the peer review process.

Areas for improvement

The ANAO made five recommendations aimed at improving: the quality of information in supporting systems; enterprise-wide assurance arrangements for the implementation of DSPF Control 23.1; PSPF and DSPF reporting on system authorisation; the advice provided to the minister; and compliance with authorisation requirements. One opportunity for improvement was identified, in relation to documenting the extent to which operational impacts have factored into the decision to authorise systems.

3.1 Fit-for-purpose governance, monitoring, and reporting arrangements support Defence to demonstrate the effective implementation of its ICT assessment and authorisation framework. Sound arrangements: are commensurate with the scale, scope, and risk of the activity; consider the available sources of data; and are responsive to the outcomes and findings from previous review activities.

3.2 In September 2021, Defence commenced an ICT inventory project to develop a 'comprehensive knowledge base of all current Defence Portfolio ICT systems, networks, applications and services'. In this context, Defence's governance and organisational arrangements should be geared to providing senior leadership with comprehensive oversight of the status of Defence's ICT security authorisations across all systems, including at the enterprise level.

Has Defence established fit-for-purpose governance, monitoring and reporting arrangements to oversee implementation of its framework and compliance with requirements?

Defence's data indicates that the obligations of System Owners to obtain and maintain the authorisation of their systems are not being fulfilled.

Defence self-assesses and reports annually on its compliance with PSPF Policy 11 and has established governance and internal reporting requirements for DSPF controls, including DSPF Control 23.1 *ICT Certification and Accreditation.* Deficiencies in Defence's reporting include that:

- Defence has not reported on the authorisation status of ICT systems at an enterprise level since 2018–19 in its PSPF and DSPF reporting (a key indicator of compliance against DSPF Control 23.1 and PSPF Policy 11);
- Defence's PSPF and DSPF reporting is not consistent with, and does not reflect, other information available within Defence on the assessment and authorisation of its ICT systems; and
- Defence has not complied with the DSPF requirement to provide individual Control Owner reports to the Defence Security Committee since 2019–20.

Defence has not briefed the minister on its ICT assessment and authorisation activities in the last three years. In September 2019, the minister requested that Defence include a metric on the reduction of unapproved systems in an 'ICT reform stream report'. Defence did not address this request.

3.3 Protective Security Policy Framework (PSPF) Policy 11 *Robust ICT systems* requires that a decision to authorise a system must be based on the Information Security Manual's (ISM) six-step risk-based approach to cyber security. Step six of the ISM's approach outlines the requirement for entities to monitor authorised systems, including regular reviews of security controls to ensure they remain fit-for-purpose, and to undertake re-authorisation where required.

3.4 Defence Security Principles Framework (DSPF) Control 23.1 *ICT Certification and Accreditation* establishes the responsibility for System Owners in 'obtaining and maintaining' the authorisation of their systems. It also outlines a requirement for systems to be re-authorised when specific conditions are met, including when new or emerging threats are detected, security measures are not operating as planned, and when the system's authorisation expires.[73] Defence's

73 The Defence Security Manual (DSM), which was replaced by the DSPF in July 2018, included additional requirements that were not retained after the introduction of the DSPF. Under the DSM, System Owners were required to undertake annual system reviews and provide those reviews to the Assessment Authority for a risk assessment to be conducted to determine whether re-authorisation was required.

The May 2024 updated DSPF Control 23.1 (see paragraph 2.6), does not specify re-authorisation conditions, and states that re-authorisation is based on 'triggers and timeframes set by the Authorising Delegate.' This is not consistent with Defence's Assessment and Authorisation Framework, which requires systems to be re-authorised when one or more of the ten specified conditions are met (see a list of the conditions at Box 1 below paragraph 3.91).

assessment and authorisation process (discussed at paragraphs 2.53–2.73) does not mandate any specific processes for ongoing monitoring of ICT systems after authorisation.[74]

System authorisation data

3.5 Defence's May 2020 internal audit into the *Certification and Accreditation of Defence ICT Networks* found that 44 per cent of ICT systems recorded by the Defence Cyber and Information Assurance Branch (DCIAB) had an expired authorisation status.[75] The audit recommended, among other things:

- better ongoing management of networks and systems using the capability of Defence's ICT authorisation management system to ensure the accuracy and currency of data;
- obtaining visibility of active systems across Defence to determine whether they have been authorised, and enable proactive management of re-authorisation, where required;
- requesting reporting from the Defence Finance Group (DFG) on Group and Service ICT procurement as a means to identify systems which have not been authorised[76]; and
- obtaining regular confirmation from System Owners that there have been no changes that would trigger a need for a re-authorisation. [77]

74 Defence's guidance in relevant policy documents is not well-aligned and indicates that ongoing or continuous monitoring activities are optional and decided at the individual system level. At June 2024, the key template to support these activities has not been developed. For example:

- Defence's Assessment and Authorisation Framework, released in May 2024 (see paragraphs 2.49–2.51) requires the completion of a Continuous Monitoring Plan and states that 'Actions to support the monitoring of cyber threats, security risks and controls relating to the system and its operating environment should be outlined in the Continuous Monitoring Plan'.
- As at June 2024, the Cyber Security Assessments and Authorisation intranet guidance page states that the Continuous Monitoring Plan template is 'under development'.
- As noted at paragraph 2.62, Defence's intranet portal process for lodging its ICT authorisations (discussed from paragraphs 2.53 to 2.71) also notes that the Continuous Monitoring Plan template is 'pending' and states that it is a document that 'may be required depending on the nature and complexity of the system'.

75 Two previous internal audits in November 2019 and April 2020 also identified 'risks associated with the design of the certification and accreditation process' including: not conducting assessments of the effectiveness of system controls; a reliance on system owners identifying the need for authorisation; and instances where systems may be live prior to the completion of the authorisation process. These internal audits were *Portable Electronic Device Monitoring Controls* (November 2019) and *Logical Security Controls* (April 2020).

76 In response to the internal audit, DCIAB stated that it would 'develop procedures to support regular reporting from Defence Finance Group (DFG) to identify groups and services procuring ICT hardware and software' by November 2020. Defence subsequently advised internal audit in October 2023 that the DFG data 'was found to provide no insights of masked/hidden system/network purchases and both CIOG finance and ITSA agreed it was not worth pursuing further'. Defence advised the ANAO in January 2024 that:

> CISO [Chief Information Security Officer] has decided to revisit this as there is now an Inventory System … to associate Hardware and Software expenditure to a registered/known ICT system. This offers the opportunity of identifying any gaps/anomalies in expenditure on ICT compared to known and registered systems, more likely than in 2020/21 … Following the Gap Analysis, JCG [Joint Capabilities Group], DFG and DDG [Defence Digital Group] will determine and agree on what (if any) ongoing reporting process will be established.

77 In response to this finding, DCIAB stated that it would introduce 'Functionality to prompt regular System Owner contact and updating of system certification records, including assurance of control implementation in response to a PICTA'. Defence advised the ANAO in June 2024 that 'Functionality exists to prompt System Owners of pending authorisation expiry … however there are no automated checks to either assure control implementation or prompt System Owners to review.'

3.6 Defence agreed to the recommendations and proposed to address them partly through conducting an inventory of Defence ICT systems and the introduction of an updated ICT authorisation management system.[78]

Inventory of Defence ICT systems

3.7 Throughout 2019–20, concerns regarding Defence's use of unauthorised systems were raised in at least three internal committee meetings as follows.

- In July 2019, the Defence Audit and Risk Committee (DARC) discussed ICT issues identified in an internal audit report[79] including a 'lack of control over systems and applications that are not managed by the CIO Group'. The DARC noted that it is 'the unknown risk that [these systems] may pose for Defence that is of concern'. The DARC requested that the Chief Information Officer Group (CIOG) conduct a stocktake of ICT systems to establish the number and types of these systems, who is responsible for them and identify any risks that they may pose to Defence.[80]
- At a Defence Committee meeting in September 2019[81], the minister was advised of a lack of awareness of unapproved systems within Defence and the vulnerabilities that unapproved systems create. The minister requested that Defence include a metric on the reduction of unapproved ICT systems in an 'ICT reform stream report'. The Defence Committee recorded this request as an action item for the Chief Information Officer to include a metric on the reduction of unapproved systems in 'ICT stream reporting'. Defence advised the ANAO in August 2024 that this action item was consolidated with the other requests from committees outlined in paragraph 3.7, resulting in Defence undertaking an inventory of Defence ICT systems (see paragraph 3.8). There is no evidence that the reporting metrics requested as per the original action item were implemented, or that the action item was closed through the Defence Committee.
- In January 2020, the Enterprise Business Committee (EBC) requested CIOG advice on 'the entities outside of CIOG that have management responsibilities for any aspect of the Defence ICT network, their scope, risks and major actions underway'.

3.8 In September 2021, Defence's Head of ICT Operations (HICTO) directed work to commence on an inventory of Defence ICT systems as a means to:

78 The internal audit, along with Defence's response to the recommendation was presented to the Defence Audit and Risk Committee in July 2020.

79 The internal audit was *Cyber Security and Intrusion Incident Management Strategy* (October 2019). One of the findings in the report was that 'Enterprise-wide accountabilities for ICT systems and cyber security should be refined and enforced'.

80 Between May 2020 and July 2023, the Chief Information Officer (CIO) provided the DARC with quarterly progress updates on the Defence ICT inventory project. In a March 2023 update, it was noted that ICT systems sitting outside of CIOG control continued to be identified. A detailed paper outlining the challenges and risks associated with the establishment of systems outside the proper approval process was requested by the DARC. To address this request, the CIO presented a paper to the DARC in July 2023, outlining the controls in place to 'prevent the proliferation of unapproved … ICT' including ICT governance committees and DSPF Control 23.1. The paper also outlined challenges including that 'Defence's current operational environment limits its ability to provide a dedicated testing regime to check compliance'.

81 The Defence Committee is the senior most committee in Defence. The November 2023 Defence Committee Charter states that the committee 'is responsible for setting top-level organisational goals and driving delivery of the Department's commitments to Government and the community.'

- develop a 'comprehensive knowledge base of all current Defence Portfolio ICT systems, networks, applications and services' including their authorisation status and authorisation expiry date;
- identify any risks that may exist across the system portfolio; and
- enable the ongoing effective governance and management of Defence Portfolio ICT systems.[82]

3.9 The inventory project has identified and recorded a range of ICT systems across the Defence portfolio.[83] Systems have been categorised and recorded under three broad definitions:

- Information Technology (IT) — 'Systems that manage the creation, processing, presentation and storage of information';
- Operational Technology (OT) — 'Systems that exist with the main purpose of aiding an effort that accomplishes a physical task'; and
- Other — 'Any other ICT system that can't be placed in a category'.

3.10 The definition adopted by the inventory project for 'IT systems' aligns with the DSPF requirement for systems that process, store, or communicate official information to be authorised.[84] 48 per cent of systems recorded in the inventory list were classified as 'IT systems'. Of these, 89 per cent did not have a recorded authorisation status. Of the systems that had an authorisation status recorded, 73 per cent were recorded as 'Active'; 9 per cent were recorded as 'No accreditation'; 9 per cent were recorded as 'Expired'; 6 per cent were recorded as 'New in progress; 2 per cent were recorded as 'In re-accreditation'; and 2 per cent were recorded as 'Not required'.[85]

3.11 In April 2023, a brief was provided to the Chief Information Security Officer (CISO) noting that the inventory system was 'experiencing user reticence through a native user interface that is unintuitive and provides information inconveniently.' The brief outlined options for migrating inventory data to Defence's ICT authorisation management system to reduce the risk of poor

82 In its response to the May 2020 *Certification and Accreditation of Defence ICT Networks* internal audit, CIOG advised that the ICT inventory project was estimated for completion in December 2021. As at April 2024, Defence's intranet states that its inventory system is an 'enduring capability'. Defence advised the ANAO in June 2024 that the ICT inventory system 'is due to be finalised for system owners to access and update their information by mid-July 2024' and would then 'transition … into sustainment by November 2024.'

83 This includes systems that were allocated to a 'Capability Manager' outside of Defence including: Department of Veterans' Affairs; Australian War Memorial; Defence Housing Australia; Army and Airforce Canteen Service; Australian Strategic Policy Institute; Australian Signals Directorate; RAAF Welfare Recreational Company; RAAF Welfare Trust; and RAAF Welfare Veteran's Residences Trust Fund. Fifty per cent of systems recorded in the inventory list did not have an allocated 'Capability Manager'.

84 The Assessment and Authorisation Framework (see paragraphs 2.49–2.51) defines OT systems as a subset of ICT systems and states that 'Where there is uncertainty of whether a system is required to undergo Assessment and Authorisation, the [Cyber Security Assessments and Authorisation] Directorate [within the Defence Cyber and Information Assurance Branch] is to be contacted to provide further advice.'

85 The total of these figures adds up to 101 per cent due to rounding. Defence's ICT inventory data was compiled by consolidating existing Defence inventories and data sources, and through consultation with relevant Defence personnel. Defence advised the ANAO in June 2024 that PwC was contracted from August 2020 to December 2022 to develop and compile Defence's ICT inventory and PwC (Scyne Advisory) was contracted in September 2023 to migrate the inventory data into the Defence's ICT authorisation management system and deliver final operating capability by October 2024.

stakeholder adoption and to improve integration with the management system's data. Defence migrated the inventory data into Defence's ICT authorisation management system in July 2024.[86]

Defence's ICT authorisation management system

3.12 Defence's system for progressing, recording and managing ICT system assessments and authorisations was introduced in August 2019, as part of Tranche 1 of the Governance, Risk and Compliance (GRC) project. The GRC project fell under a broader 'multiyear Security Enhancement program' that commenced in 2017.[87] The system was upgraded as part of Tranche 2 of the GRC project in March 2022.[88] Defence advised the assistant minister in October 2022 that the GRC initiative had been delivered.

3.13 Defence's ICT authorisation management system includes fields to record key system information including: system authorisation status and authorisation date; authorisation expiration date; residual risk rating[89]; Business Impact Level (BIL); Authorising Officer; Group/Service; and System Owner. The system also allows for key supporting documentation, such as the System Security Plan (SSP), to be uploaded as part of the system record.[90]

3.14 As noted in paragraph 3.10, approximately 48 per cent of the systems identified through Defence's inventory project are IT systems that 'manage the creation, processing, presentation and storage of information'. Of these IT systems, 5 per cent had been recorded in Defence's ICT authorisation management system (as at June 2024).

Data quality

3.15 ANAO analysis of Defence's ICT authorisation management system data identified data quality issues, indicating weaknesses in the processes established to ensure that complete and accurate data is recorded in the system. Not all data fields have been consistently populated. Responsibility for completing these fields is allocated across multiple roles, including the System Owner, Security Analyst and Security Assessor, throughout the assessment and authorisation process. Table 3.1 outlines key fields and the extent to which data has been recorded against those

86 The inventory data is accessible through Defence's ICT authorisation management system as a separate data set. As such, analysis of the inventory data (paragraph 3.10) is discussed separately to the ICT authorisation management system data (paragraphs 3.15–3.24).

87 Prior to the implementation of the ICT authorisation management system, Defence used Microsoft SharePoint to manage assessment and authorisation activities. Defence advised the ANAO in June 2024 that the final cost for the system under Tranche 1 was $9.9 million.

88 One element of the upgrade to the system included the addition of risk and control libraries. The system's control library includes ISM controls from various versions of the ISM between April 2013 and September 2021. While the project closure report is signed off by a Project Manager and Senior Responsible Officer, the document's status is recorded as a draft.

The project closure report for the upgraded system noted that the project cost for the upgrade was $5.06 million. The closure report also noted that the upgrade would deliver benefits including: '[i]ncreased agility in cyber security decision making'; '[m]ore effective dependency management and reporting on cyber security capabilities'; and '[i]ncreased efficiency of cyber security service delivery through reduction in duplication and inconsistency'. A May 2024 Control Owner report (see paragraphs 3.61–3.62) found that the implementation maturity of DSPF Control 23.1 had decreased due, in part, to the ICT authorisation management system's lack of maturity.

89 Residual risk is the risk that remains after controls have been implemented and is included in the Decision Brief to support the Authorising Officer's authorisation decision (see paragraph 2.68).

90 Supporting SOPs for Defence's ICT authorisation management system instruct System Owners to add relevant documentation to the system, including the mandatory System Security Plan.

fields for the systems that have been documented in Defence's ICT authorisation management system.

Table 3.1: Completeness of fields across the IT systems recorded in Defence's ICT authorisation management system, as at 30 July 2024

System field	Field completion (%)
Authorisation status	100
Authorisation date	56[a]
Authorisation expiration date	49[b]
Residual risk rating	99.9
Business Impact Level	99.9[c]
Authorising Officer (Accreditation Authority)	31[d]
Group/Service	92
System Owner	74
System Security Plan	19[e]

Note a: Of these systems, 1 per cent had an authorisation date that was prior to the recorded Risk Assessment date. As discussed at paragraph 2.71, a Risk Assessment is provided to the Authorising Officer prior to an authorisation decision being made. Four per cent of systems had an authorisation date of 30 June 2099. For the 4 per cent of systems with authorisation dates of 30 June 2099, Defence advised the ANAO in May 2024 that, prior to the implementation of the upgraded ICT authorisation management system, the authorisation date was a mandatory field once a system had been assigned for assessment, and that 'Cancelling the system after this required entering a value'. Defence further advised that 'None of the … systems with accreditation dates falling in 2099 represent current accreditations.'

Note b: Of these systems, 0.4 per cent had authorisation expiry dates more than 75 years into the future. Authorisations for 0.3 per cent of systems (all granted in 2017) were for 4.01 years, exceeding the three-year maximum authorisation period available under the Defence Security Manual (DSM), which was in effect at the time. The DSM stated that 'Accreditation certificates **must** [emphasis in original] expire after three years.'

Note c: Of these systems, 90 per cent had a Business Impact Level rating of 'Unknown'.

Note d: Of these systems, 7 per cent had recorded the Authorising Officer as the 'Chief Technology Officer / Chief Information Security Officer'. For 18 per cent of those systems the CISO was also the Assessment (Certification) Authority. Under the DSPF, Assessment Authority responsibilities include providing recommendations to the Authorising Officer.

Note e: The May 2020 internal audit, *Certification and Accreditation of Defence ICT Networks,* assessed a sample of five Defence systems and found that the System Overview Document (which was superseded by the System Security Plan in January 2023) was missing for three systems.

Source: ANAO analysis of Defence data.

3.16 Defence's data suggests that the number of system authorisations it conducts annually has been progressively increasing (by an average of 50 per cent each year).

- The number of Defence systems authorised in 2023 was 744 per cent higher than the number authorised in 2012.
- The average number of Defence systems authorised each year from 2012 to 2023 equates to 0.2 per cent of the total number of 'IT systems' identified through Defence's ICT inventory project.
- The number of systems authorised by Defence in 2023 was equivalent to 0.3 per cent of the 'IT systems' identified in the inventory project.

System authorisation status

3.17 Many of the ICT systems recorded did not have an 'Active' authorisation status.[91] Of the systems recorded in Defence's ICT authorisation management system as at 30 July 2024, the authorisation statuses were: 'Expired' (26 per cent); 'No accreditation' (21 per cent); 'Active' (12 per cent); 'New in progress' (27 per cent); and 'In re-accreditation' (14 per cent). Of those systems with an 'Active' authorisation status, 30 per cent had an authorisation expiry date that had passed (at the system report date of 30 July 2024).

3.18 Air Force Standing Instruction 05-02 *Cyberworthiness, Certification and Accreditation* requires the Air Force to maintain a register of Air Force systems and their assessment and authorisation status. Of the systems identified on the Air Force list as at February 2024: 72 per cent were not authorised; 20 per cent were either fully or provisionally authorised; 5 per cent had authorisations in progress; and 3 per cent had no authorisation status recorded. Of the systems that were recorded as either fully or provisionally authorised, the authorisation expiry date had passed for 55 per cent (as at 30 April 2024). Defence advised the ANAO in August 2024 that 'work to consolidate [Air Force] accreditation status data with [Defence's ICT authorisation management system data] is yet to be planned and resourced.'

3.19 Defence's ICT authorisation management system data (see Appendix 3) shows that, for systems with a risk rating of 'low' to 'significant', the most common authorisation status is 'Expired'. Of the 0.09 per cent of systems with a residual risk rating of 'Extreme', half of those had an authorisation status of 'No accreditation' and the other half had a status of 'Expired'. Of the systems recorded in Defence's ICT authorisation management system, 37 per cent had been allocated a residual risk status of 'Unknown'.

3.20 As noted at paragraph 3.17, 47 per cent of systems were recorded with a status of either 'Expired' or 'No accreditation'. For these systems, the 'System Operation Status' was recorded as: blank (85 per cent); 'operational' (8 per cent); 'development' (5 per cent); 'retired' (2 per cent); and 'commissioned' (1 per cent).[92] Due to the number of blank fields, the extent to which unauthorised systems remain operational is unclear. The ISM six-step process includes requirements for the decommissioning of systems once they are no longer operational.

91 Defence advised the ANAO in June 2024 that the authorisation status definitions are: Expired — 'System had achieved full or provisional accreditation that has passed its recorded expiration date'; No accreditation — 'system has been removed from an active workflow through either task cancellation or system deprecation'; Active — 'System has achieved full or provisional accreditation and is operating within its recorded accreditation period'; New in progress — 'System has not previously achieved full or provisional accreditation, and is being assessed for the first time'; and In re-accreditation — 'System had achieved full or provisional accreditation, and a reassessment has been initiated'.

92 The total of these figures adds up to 101 per cent due to rounding.

3.21 The ICT authorisation system records for systems with a 'New in progress' status had not been updated for an average of 388 days as at 30 July 2024, indicating that the assessment and authorisation process had not progressed on Defence's ICT authorisation management system during that time. Of the systems with a 'New in Progress' status, 34 per cent had not been updated in over 600 days, including 5 per cent that had not been updated for 1,035 days.[93] Defence analysis conducted in 2021 found that requests for assessment and authorisation took an average of 285 days to be completed during the 12 months up to September 2021.

3.22 In September 2020, DCIAB conducted a review of its staffing levels in response to an internal audit into Defence's assessment and authorisation arrangements. The review found that 'on average the team is operating above 100 per cent utilisation', resulting in delays to system assessments, responding to enquiries, and project engagement, as well as impacting staff wellbeing. Defence advised internal audit in December 2021 that 'The proposed solution was assessed internally and, due to CIOG ASL [Chief Information Officer Group Average Staffing Level] pressures and limitations, plus in the interest of expediency, the Defence CISO elected to address the staffing deficiency with a contracted workforce.'

System re-authorisation

3.23 Defence's intranet states that non-urgent authorisation requests may take up to 180 days. Defence's intranet also states that:

> if Certification Management (DCIAB) has been engaged and a current task exists to commence a re-Certification/Accreditation activity, the existing Accreditation will remain valid until the activity is completed and a decision received from the appropriate Accreditation Authority on the re-Accreditation request.

3.24 At 30 July 2024, 14 per cent of systems in Defence's ICT authorisation management system had a status of 'In re-accreditation'. On average, the records for these systems had not been updated for 255 days. Three per cent of the systems with a status of 'In re-accreditation' had not been updated for 1035 days.[94] This indicates that the re-authorisation process had not progressed on Defence's ICT authorisation management system during that time. Further, 68 per cent of the systems undergoing re-authorisation had passed their authorisation expiry date as at 30 July 2024. One of these was Defence's ICT authorisation management system itself which, as at 9 August 2024, had an authorisation status of 'In re-accreditation'. The system's authorisation expired on 2 March 2023.[95]

93 The ICT authorisation management system records showed that these systems were last updated by a 'Data Feed Service' on 29 September 2021. Defence advised the ANAO in June 2024 that:

> [the] Data Feed Service automates the import, export, and modification of data between [the ICT authorisation management system] and other systems … The dates of the records … reflect the initial data import from the ICT2271 Tranche 1 build of [the ICT authorisation management system] to Tranche 2 … In the case that referenced systems have not been updated since September 2021, without visibility of the systems assessed, it is assumed that these systems are either deprecated or cancelled.

94 The ICT authorisation management system records showed that all of these systems were last updated by a 'Data Feed Service' on 29 September 2021. See Defence's explanation for this at footnote 93.

95 The system's Decision Brief records the system's authorisation date as 2 March 2022, and notes that authorisation was to last for one year. This would result in system authorisation expiry on 2 March 2023. The system's authorisation expiry date is recorded as 6 March 2023 in the ICT authorisation management system.

Recommendation no. 4

3.25 The Department of Defence develops and implements processes to ensure that information entered into its ICT authorisation management system is complete, accurate, and supports effective monitoring of ICT system authorisations.

Department of Defence response: *Agreed.*

3.26 *The A&A [Assessment and Authorisation] Improvement Program will include remediation of deficiencies with the Cyber platform and ensure associated processes and workflows are efficient and support effective monitoring and control of ICT systems authorisations.*

Control 23.1 assurance arrangements

3.27 The DSPF states that DSPF Control Owners are responsible for managing, monitoring and reporting on the implementation of their controls across Defence. Control Owners may establish 'assurance frameworks' to delegate the responsibility for control implementation and control reporting to Group Heads, Service Chiefs, Commanders and Managers of business units.[96] Defence advised the ANAO in January 2024, that 'there has been no specific assurance framework established with the Control Implementers to measure the effectiveness of DSPF Control 23.1.'

3.28 Internal audits in 2019 and 2020 (see paragraph 3.5) found deficiencies in the design of Defence's assessment and authorisation process, including that there were no arrangements in place to: assess the effectiveness of system security controls; ensure system owners implement recommendations made through the assessment process; and ensure changes that trigger re-authorisation requirements are identified and actioned by system owners.[97]

3.29 In September 2020, the Defence Security Committee (discussed further at paragraphs 3.52–3.65) was advised that:

> Control Owner awareness of their responsibilities and accountabilities under the DSPF, and their engagement with the implementation of their Control is not sufficient to assure that Defence is adequately managing security risks. In this reporting period [2019–20], Control Owners reported they do not have sufficient oversight of their DSPF Control to adequately govern the implementation of their policy.

3.30 Consistent with this advice, an internal Defence review in 2022 found that Control Owners do not have sufficient information to make 'measurable improvements to their existing controls'

96 The DSPF also requires Groups and Services to appoint Executive Security Advisers (ESA) to support Control Owners' analysis of their security environment. Defence advised the ANAO in March 2024 that 'no assistance has been provided by any ESA with Control 23.1 over the course of the last few years. This is primarily due to the control owner being the ITSA who resides within the CISO organisation and has a team to support him/her.'

97 In response to the audit findings, CIOG advised internal audit in October 2020 that it would, among other things, seek a 'one-off situational report' and subsequent quarterly reporting from Air Force and the Australian Defence Training Simulator Centre to confirm that relevant systems were authorised during the reporting period. Defence advised the ANAO in March 2024 that it was unable to find evidence that this reporting took place.

and that it was 'difficult for Defence to make broad judgements about the extent to which the DSPF is providing sufficient mitigation.'[98]

3.31 Defence advised the ANAO in June 2024 that:

> Responsibility to monitor the triggers for reauthorisation rests largely with the System Owner's organisation via normal system and business management practices … Defence understands this is currently an area for improvements as there are insufficient automated facilities to assist the System Owner (and Accreditation Authority) to meet their obligations.
>
> Integrated Continuous Assurance (ICA) functionality originally scoped for [Tranche 2 of the GRC project] was expected to enable a large portion of this functionality however it was de-scoped out of [Tranche 2]. As such, [Defence] is presently pursuing this functionality as part of its monitoring improvement strategy.

Service level assurance and monitoring arrangements

3.32 As discussed at paragraph 2.26, Army, Navy and Air Force have each issued policies, instructions or directives to support compliance with DSPF Principle 23 and Control 23.1. These documents include assurance and monitoring requirements for ICT system assessment and authorisation.

Army

3.33 The Chief of Army issued the Army Standing Instruction (Protective Security) in August 2021 (updated November 2023), which requires units to conduct annual cyber self-assessments to 'normalise the conduct of cyber security within units and provide a means to monitor the maturity of unit cyber security.'[99] The self-assessments include checking that: authorisation documentation is in place; authorisation is current; and whether any changes to the system may impact the system's authorisation status.

3.34 Army provided the ANAO with examples of four completed self-assessment reports from 2022 and 2023. These reports contained a number of incomplete fields or issues. For example: one report did not confirm that authorisation documentation was in place for all relevant systems[100]; two indicated that relevant authorisations had expired; two had not documented whether an assessment of system changes (that could impact authorisations) had occurred; and two reports

98 Defence advised the ANAO in June 2024 that it was 'unable to identify if the Secretary or CDF have been briefed on the DSPF control issues raised by the 2022 internal review.'

99 To support the conduct of assurance activities, Army has developed a three-tiered Compliance and Assurance Framework. Unit self-assessments fall under Tier 1 of the framework. Tier 2 and Tier 3 assurance activities are conducted at the 'formation' and Army levels respectively. 'Formation' refers to groups comprised of multiple 'units'. Defence provided results of Tier 3 assurance activities conducted in 2023–24. The assurance activity sought confirmation of system 'certification' only. Supporting guidance stated that 'Certification provides the authorising officer information with [sic] the security posture of a system and allows them to make an informed decision on the security risk of authorising a system to operate' and units are to maintain a 'repository for all documentations and other relevant information necessary for the management of … the entire life cycle of the IT systems'. The assurance activity results show that, of the 43 units selected for testing: 16 passed; 2 did not pass and remediation action was planned; 5 were not tested (due to unavailability of staff or insufficient time); and for 20 units the test was not applicable as the unit did not have, or were not responsible for, ICT system certification.

100 The unit had selected 'N/A' and stated that 'we do not hold the accreditation documentation in the unit. External providers maintain the systems.'

had not been signed by all required officers.[101] Defence advised the ANAO in June 2024, that '[n]o specific follow-up activities were conducted in response to issues raised within the reports.'

Navy

3.35 The Navy Cyberworthiness Policy, released in August 2022, requires that a Cyberworthiness Department Managed Audit (DMA) is conducted prior to a capability being released following a period of maintenance, and at least every two years thereafter. The DMA includes assessing whether authorisation documentation is available and recorded in the Configuration Status Account (CSA) 'as proof … ICT systems are certified and accredited'. Navy provided the ANAO with seven audit reports completed over 2022 and 2023.

3.36 All seven reports found deficiencies in authorisation documentation and five reports identified systems that had not been authorised. The reports' findings included that 'lack of certification and accreditation is beyond the ability of [Navy] to address'; 'it is almost impossible for [Navy] to be compliant and have a robust system when Cyberworthiness is yet to be achieved for the entire Group'; and 'until the Navy Cyberworthiness is in a more mature state all requirements of the Cyber DMA will not be possible to be met.' Three reports stated that release of the capability should not be delayed or prevented.

3.37 The reports' findings are consistent with advice to senior Navy personnel between October 2021 and June 2022, which identified a lack of authorisation of Navy systems in accordance with the DSPF. The advice noted that Navy considered it 'unreasonable' to authorise all systems in the short-term, however authorisation of all systems remained Navy's long-term goal.

3.38 The advice included a list of 'priority' unauthorised systems, each with a Business Impact Level (BIL) of 'Extreme' and requested agreement from Navy to 'initiate the certification and accreditation process as soon as possible.'

3.39 The relevant senior personnel responded to the advice in June 2022 agreeing the need to authorise the identified systems. The response also stated that the relevant business area did not 'have required skillsets, expertise and capacity to initiate and manage the accreditation process requirements for all the systems outlined'. The response proposed that the matter be raised at the relevant Navy Review Board. The review board referred the issue to the relevant Governance Board in July 2023, which decided that an 'enterprise approach to cyberworthiness needs to be adopted, resourced and funded appropriately', and appointed the Director General of Navy Intelligence and Information Warfare (Director General NIW) to take the lead with this initiative.

3.40 A minute provided to the Director General NIW in October 2023 outlined the board's decisions and stated that '[o]f the … Navy owned ICT and OT maritime materiel and support systems, installed … less than 1 per cent have achieved accreditation or have an extant system CwMP [Cyberworthiness Management Plan]'.

3.41 In March 2024, the Director General NIW advised the Navy Review Board that a cyber evaluation and management tool was being developed to support the assessment and authorisation of Navy platforms. The board was advised that the tool will be trialled to assess the

101 The report is to be authorised by the relevant IT Security Officer (ITSO), Commanding Officer (CO) and IT Security Manager (ITSM).

cyber risk, current controls and mitigation strategies of a Navy capability, in order for the capability to be considered for authorisation in November 2024.

3.42 Defence advised the ANAO in June 2024 that the systems identified in the Navy advice had not been authorised and that six of the seven capabilities subject to the DMA were released for operational use prior to their ICT systems being authorised. This is not consistent with PSPF Policy 11 which requires that entities must only process, store or communicate information and data on an ICT system that has been authorised to operate.

Air Force

3.43 Air Force instruction AC SI(OPS) 05-50 *Cyberworthiness of Air Force Command, Control, Communications, Computers and Intelligence Systems* requires the audit and oversight of 'cyber practices, systems compliance and [Air Force security module] reporting on behalf of the Air Commander.' Air Force provided a list of Air Force ICT systems (see paragraph 3.18) which included analysis of the number, risk level and authorisation status of the systems.[102] The documents provided did not include evidence of auditing or oversight of assessment and authorisation requirements.

3.44 Briefings to the Air Commander Australia[103] between January 2018 and September 2019 identified that:

- approximately 3 per cent of Air Force systems had achieved authorisation, and that meeting a CDF direction for all systems to be authorised by September 2018 was 'unrealistic';
- there was a 'lack of awareness of accreditation responsibilities in Air Command' and an approved Air Force instruction outlining authorisation requirements; and
- the Air Commander provided approval for the operation of an Air Force training system without ICT authorisation for the period 11 March 2019 to 29 March 2019, for the purposes of operational testing and evaluation.

Recommendation no. 5

3.45 The Department of Defence:

(a) implement enterprise-wide assurance arrangements to support the effective implementation of DSPF system authorisation requirements; and

(b) implement arrangements to ensure that deficiencies and non-compliance identified through Service assurance activities relating to system authorisations are addressed and rectified.

Department of Defence response: *Agreed.*

102 Defence also provided: a December 2023 email from an Air Force officer to Air Command requesting that a decommissioned system be removed from the Air Force security module list; a December 2023 vulnerability assessment of air refuelling tankers; and records from the March 2024 Air Force Risk Committee.

103 The Air Commander Australia is responsible to the Chief of Air Force for effectively preparing air combat forces.

3.46 *Defence will review and enhance first and second lines of assurance, to ensure effective implementation of DSPF system authorisations, as part of the process improvement line of effort in the A&A [Assessment and Authorisation] Improvement Program.*

PSPF self-assessments

3.47 Under the PSPF, all non-corporate Commonwealth entities must report on their self-assessed level of maturity against PSPF requirements to their portfolio minister and the Department of Home Affairs each financial year. The DSPF outlines Defence's obligation for annual reporting to government on PSPF compliance, and establishes supporting governance and reporting arrangements for DSPF Controls, including Control 23.1, through regular Control Owner reporting.

3.48 PSPF Policy 5 requires entities to conduct their self-assessment of each PSPF policy against a four-point rating scale: Maturity Level 1 – Maturity Level 4. These maturity levels are assigned descriptors: 'partial', 'substantial', 'full' and 'superior' respectively. Prior to October 2022, these maturity levels were called: 'ad hoc', 'developing', 'managing' and 'embedded', with descriptors 'partial', 'substantial', 'full' and 'excelled' respectively.

3.49 The PSPF self-assessment report includes a section to outline the rationale for the selected maturity level for each policy, as well as a detailed assessment section with questions regarding compliance against key aspects of each PSPF policy. For PSPF Policy 11, question 11.2 of the detailed assessment asks entities to assess their implementation of the requirement that:

> Before processing, storing or communicating sensitive or classified information on an entity ICT system, the determining authority (or their delegate) has authorised the system to operate based on the acceptance of the residual security risks to the system and information in accordance with the Australian Government Information Security Manual.

3.50 Defence's self-assessment results for PSPF Policy 11, including extracts of relevant sections of the rationale, are outlined in Table 3.2.

Table 3.2: Defence PSPF Policy 11 maturity self-assessments

Year	Maturity level	Rationale	Implementation of Question 11.2
2018–19	Developing[a] (Level 2)	The Certification and Accreditation process ensures risks to ICT systems are identified, mitigated and/or accepted as necessary. Defence is ensuring that there are defined Governance and Functional appointments in the certification and accreditation process, with Certification and Accreditation Authorities identified for each Group or Service.[b]	Substantial[c] (Level 2)
2019–20	Developing[a] (Level 2)	Mature certification and accreditation processes are established and engaged in the early phases of the development lifecycle of new ICT systems … Assurance processes ensure appropriate levels of logging and audit, aligned to ISM requirements, are applied to all ICT systems and capabilities prior to their operational use. The certification and accreditation process ensures risks to ICT systems are identified, mitigated, and/or accepted as necessary.	Substantial[c] (Level 2)

Year	Maturity level	Rationale	Implementation of Question 11.2
2020–21	Managing[d] (Level 3)	Before processing, storing or communicating sensitive or classified information, Defence applies a rigorous certification process to all ICT systems including Defence Industry systems that process, store and/or communicate sensitive and classified Defence information.	Excelled[e] (Level 4)
2021–22	Managing[d] (Level 3)	Before processing, storing or communicating sensitive or classified information, Defence applies a rigorous certification process to all ICT systems including Defence Industry systems that process, store and/or communicate sensitive and classified Defence information.	Full[f] (Level 3)
2022–23	Maturity Level 2	Before processing, storing or communicating sensitive or classified information, Defence applies a rigorous certification process to all ICT systems including Defence Industry systems that process, store and/or communicate sensitive and classified Defence information.	Full[f] (Level 3)

Note a: The definition of 'Developing' is 'Security measures are substantially in place for ICT system development. Certification and accreditation of ICT systems in accordance with ISM technical standards is, in the majority of cases, managed when operationalised'.

Note b: As discussed at paragraphs 2.13–2.16, Authorisation Officer roles had not been fully defined for most Defence Services and Groups in the DSPF.

Note c: The definition of 'Substantial' is 'Requirement is largely implemented but may not be fully effective or integrated into business practices.'

Note d: The definition of 'Managing' is 'Security measures are applied during all stages of ICT system development. ICT systems are assessed and authorised (previously certified and accredited) in accordance with ISM technical standards when operationalised'.

Note e: The definition of 'Excelled' is 'Requirement and relevant better-practice guidance are proactively implemented in accordance with the entity's risk environment, are effective in mitigating security risk and are systematically integrated into business practices.'

Note f: The definition of 'Full' is 'Requirement is fully implemented and effective and is integrated, as applicable, into business practices.'

Source: ANAO analysis of Defence PSPF annual reports.

3.51 Table 3.2 shows that, since 2018–19, Defence has assessed that it has achieved Maturity Levels 2–3 for the requirement to authorise ICT systems before processing, storing or communicating sensitive or classified information. Table 3.2 also shows that, since 2020–21, Defence has reported that it 'applies a rigorous certification process to all ICT systems … that process, store and/or communicate sensitive and classified Defence information'.[104]

Control Owner reporting

3.52 To develop an enterprise-wide security risk view, and support PSPF annual reporting, the DSPF requires Control Owners to 'report to the DSC [Defence Security Committee] on each DSPF Principle and Expected Outcome' to provide assurance that DSPF controls are being implemented and highlight any serious security incidents, risks or events.

104 A covering brief to the CDF and Secretary in relation to the 2021–22 self-assessment noted risks in relation to the 'partial implementation of the Essential 8 across Defence's ICT environments.' As discussed at paragraphs 2.58–2.59, Defence's assessment and authorisation process includes an assessment of compliance against Essential Eight requirements.

3.53 The DSC charter states that it is 'responsible for supporting the Chief Security Officer in implementing the requirements of the Protective Security Policy Framework' and 'provides oversight on security risk management, specifically, an annual cycle of strategic security risk management planning, reporting and quality assurance'.[105]

3.54 Prior to February 2023, DSPF Control Owners were required to provide a report to the DSC on an annual basis. For the 2019–20 and 2020–21 reporting periods, Control Owner reports were completed but were not submitted individually to the DSC. Instead, the Defence Security Division 'collated Control Owner Reports into a single annual summary brief for the DSC'.[106] Neither an individual Control Owner report for Control 23.1 nor an annual summary was provided to the DSC for the 2018–19 reporting year.

3.55 In May 2022, the Chief Security Officer provided a paper to the DSC, proposing a rolling program of Control Owner reporting 'to re-align Control Owner reporting with the governance provisions of the DSPF'. As part of the rolling program, Control Owners would 'provide an annual report to the DSC on each DSPF Principle and Expected Outcome they have responsibility for' in accordance with the requirement stipulated in the DSPF.[107] The DSC agreed to the proposal.

3.56 In February 2023, the DSC endorsed a further recommendation to change the frequency of Control Owner reporting from annually to once every two years.[108] Defence advised the ANAO in June 2024 that this was to provide 'sufficient time for Control Owners to produce quality and meaningful reporting; and ensuring [there was] sufficient time in DSC meeting[s] to meaningfully review and discuss Control Owner reports.' The 'Governance and Executive Guidance section' of the DSPF was updated in March 2024 to reflect this change.

3.57 To support Control Owner reporting, Defence has developed a template that Control Owners are required to use for reporting to the Defence Security Committee.[109] The template requires Control Owners to assess Defence's implementation of DSPF Principles and assign an overall maturity rating based on the PSPF four-point scale (see paragraph 3.48). Other sections of the template instruct the Control Owner to provide information about security incidents, risk and assurance activities related to the Control.

105 Since the DSPF was released in July 2018, the Chief Security Officer has been the First Assistant Secretary of the Defence Security Division (previously called the Defence Security and Vetting Service).

106 The annual summaries and supporting papers included maturity ratings for all 42 DSPF controls, an assessment of controls with maturity ratings that have increased, decreased or have an 'adhoc' maturity rating, insights from the reporting process, risks and issues, and planned activities. Defence advised the ANAO in June 2024 that 'An executive summary was in place due to the number of Control Owner reports expected to be submitted – though evidence of this rationale is not available.'

107 The paper noted that the previous approach of not providing Control Owner reports directly to the DSC 'deprives DSC members of and control owners from an opportunity to seek further information or clarifications' and that 'Reinforcing the requirement for Control Owners to report to the DSC, will also enhance the Committee's role in providing oversight of the DSPF.'

108 Defence advised the ANAO in January 2024 that, due to the changes in control owner reporting schedules, there was no Control Owner Report for Control 23.1 submitted for the 2021–22 financial year.

109 While completion of the template is required by DSPF, a supporting May 2023 Control Owner guide states that 'the format and content for Control Owner Reporting is at the discretion of the individual Control Owner'.

3.58 In Control Owner reporting for DSPF Control 23.1 between 2018–19 and 2020–21, the implementation of DSPF Principle 23 was assigned an overall maturity rating of 'Managing', which was accompanied by the following description:

> the DSPF Principle is implemented, integrated into business practices and effectively disseminated across Defence. Defence meets all DSPF Expected Outcomes, with only occasional and minor lapses.

3.59 Further commentary in the 2018–19 and 2019–20 reports noted that:

> Assurance processes, ensuring appropriate protections for unofficial, official, sensitive or classified Defence information during processing, storage and communication, are applied to all Information Communications and Technology (ICT) systems and capabilities prior to their operational use. The Certification and Accreditation process ensures risks to ICT systems are identified, mitigated and/or accepted as necessary.

3.60 The Control Owner report for 2020–21 stated that:

> Defence's Information Assurance processes (ICT System Certification and Accreditation) is considered effective in ensuring appropriate protections are in place on Defence ICT systems prior to authorisation to process, store and/or communicate operational sensitive and classified information. The Certification and Accreditation process ensures risks to ICT systems are identified, mitigated and/or accepted as necessary.
>
> …
>
> DSPF Principle 23 and Control 23.1 outlines governance and functional appointments in terms of responsibility for the conduct of ICT systems certification and accreditation across Defence.[110]
>
> The Certification and Accreditation process incorporates checks and balances to ensure assessments remain relevant and considers emerging cyber threats.[111]

3.61 In May 2024, a Control Owner report for Control 23.1 was provided to the DSC. The maturity of Defence's implementation of DSPF Principle 23 was assessed as 'developing', with the report outlining deficiencies including that: assessment and authorisation policy was not current; Defence's ICT authorisation management system did not sufficiently support an enterprise-wide view of ICT risks; and the volume of Defence ICT systems outweighs available resources for assessment and authorisation activities.[112] As outlined at paragraph 3.16, on average, 0.2 per cent of the total number of Defence systems identified through Defence's ICT inventory project that 'manage the creation, processing, presentation and storage of information' are authorised each year.

110 As discussed at paragraphs 2.13–2.16, Authorisation Officer roles had not been fully defined for most Defence Services and Groups in the DSPF.

111 Defence advised the ANAO in June 2024 that '[i]t is unclear what the checks and balances referred to in this report were'.

Eight incidents relating to Control 23.1 were reported in 2020–21, with seven of these instances relating to systems having no authorisation or an expired authorisation. The report stated that 'further review deemed these incidents to have a minor impact to Defence and the assurance of Defence information.' The 2020–21 report also identified one risk for Control 23.1, which related to the resources available within DCIAB to meet the high demand for authorisation across Defence.

112 The report outlined actions being taken to address these issues, including updates to the DSPF, the release of the Assessment and Authorisation Framework, the establishment of a business engagement function to provide advice to stakeholders, and improvements to Defence's ICT authorisation management system.

3.62 DCIAB internal reviews of the draft 2024 Control Owner report, prior to it being presented to DSC, suggested on at least two occasions that the number of systems that had not been through the assessment and authorisation process should be included in the Control Owner report. The final version did not include those numbers. Defence advised the ANAO in June 2024 that '[a]t the time of preparing the Control Owner report, the statistics available could not be summarised into a cohesive and confident set of annualised statistics and this was therefore dropped from inclusion so as not to misrepresent or mislead the current state to the DSC.'

3.63 For the period of reporting examined by this audit, (2018–19 to 2023–24), neither Defence's PSPF self-assessment nor Control Owner reporting has included information on the authorisation status of Defence systems at an enterprise level. This information is a key indicator of compliance against the PSPF Policy 11 (and DSPF Control 23.1) requirement that entities 'only process, store or communicate information and data on an ICT system that the determining authority (or their delegate) has authorised to operate'.

3.64 Defence's reporting on its compliance with this requirement contrasts with information available in other Defence documentation, including:

- the findings of internal audits conducted in 2019 and 2020 (see paragraph 3.5);
- ICT system authorisation data (see paragraphs 3.17–3.24) which indicates that 47 per cent of systems recorded had an authorisation status of either 'Expired' or 'No accreditation';
- the findings of service-level assurance activities (see paragraphs 3.32–3.44); and
- records from various Defence committees (see paragraph 3.7) outlining concerns raised in relation to Defence's use of unauthorised ICT systems.

3.65 The lack of alignment between the information in Defence's other documentation and its PSPF and Control Owner reporting since 2018–19 raises issues around the accuracy and transparency of Defence's reporting to its accountable authority and senior leadership. Under Section 25 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), officials are required to perform their functions and discharge their duties with reasonable care and diligence. Section 26 of the PGPA Act sets out that officials are to exercise powers, perform functions and discharge their duties honestly, in good faith and for a proper purpose.[113]

DCIAB reporting

3.66 DCIAB produces weekly reports providing summaries of key issues across the branch, including updates on the assessment and authorisation status of specific ICT systems. Since DCIAB's transition from CIOG to Cyber Command in January 2024, these reports have been provided to the Commander of Cyber Command. Prior to January 2024, these reports were provided to Defence's

113 In addition, Australian Public Service (APS) employees must have regard to the following.
- Section 14 of the Australian Public Service Commissioner's Directions 2022 (dated 31 January 2022) provides that upholding the 'ethical' value in subsection 10(2) of the *Public Service Act 1999* requires the following: 'complying with all relevant laws' and 'acting in a way that is right and proper, as well as technically and legally correct or preferable'.
- Section 32 of the PGPA Act, which states that to avoid doubt, the finance law is an Australian law for the purposes of subsection 13(4) of the *Public Service Act 1999*. If the Public Service Act applies to an official of a PGPA entity, the official will be required under subsection 13(4) of the Public Service Act to comply with applicable Australian laws, which include the finance law.

Head of ICT Operations (HICTO). There have been no instances where this reporting included the number of systems that were authorised or unauthorised across Defence.

Recommendation no. 6

3.67 The Department of Defence implement arrangements to ensure reporting to senior Defence leadership on compliance with system authorisation requirements under the PSPF and DSPF is comprehensive, accurate, and based on available data.

Department of Defence response: *Agreed.*

3.68 *The A&A [Assessment and Authorisation] Improvement Program will include governance and reporting improvements that comprehensively and accurately represent the PSPF compliance status and DSPF performance.*

Reporting to the Minister for Defence

3.69 In January 2024, Defence advised the ANAO that:

> no specific briefings have been provided to the Defence Minister on either Certification and Accreditation (C&A) or Assessment and Authorisation (A&A) in the last three years.

3.70 Defence has provided the minister with annual briefings in relation to its PSPF self-assessments. None of the briefings prepared during the period examined by this audit (since 2018–19) have contained any information about the authorisation status of Defence ICT systems.[114]

3.71 As noted at paragraphs 3.47–3.68, deficiencies were identified in Defence's PSPF and DSPF reporting, including not disclosing the extent of recorded unauthorised systems across Defence (a key indicator of compliance against the requirements of PSPF Policy 11). This same information, and the risks it poses to the Department, has also not been reported to the minister. This raises questions as to whether the minister has been kept sufficiently informed of key issues in relation to assessment and authorisation. Under Section 19 of the PGPA Act, the accountable authority of a Commonwealth entity is required to keep the responsible minister informed of the activities of the entity, including any 'significant issues' that may affect the entity.

Recommendation no. 7

3.72 The Department of Defence:

(a) ensures that relevant ministers are provided with timely and accurate advice on key issues and risks relating to Defence's ICT security authorisations and its compliance with the PSPF; and

114 The 2018–19 PSPF self-assessment brief advised the minister of ICT security weaknesses as a result of remaining legacy ICT. PSPF self-assessment briefs in 2021–22 and 2022–23 advised the minister of partial implementation of the Essential Eight. Defence also provided the ANAO with briefings to the Assistant Minister for Defence in relation to Defence's 2022 ICT Strategy and aspects of the Governance, Risk and Compliance Project. The 2022 ICT Strategy brief and PSPF self-assessment briefs for 2021–22 and 2022–23 were not signed by the minister. Defence advised the ANAO in June 2024, that it 'is unable to locate signed versions of the briefs'.

(b) provides regular (at least annual) updates to relevant ministers to support oversight for improvements to its assessment and authorisation policies, frameworks and processes.

Department of Defence response: *Agreed.*

3.73 *The A&A [Assessment and Authorisation] Improvement Program governance improvements will include enhancements to reporting to ensure the Defence Enterprise Committee structure and Defence Ministers have timely visibility of ICT security authorisation performance, key issues and risks. This will include, at a minimum, an annual update to relevant Ministers to support their oversight of A&A policies, frameworks and process improvements.*

Have selected Defence ICT systems been authorised and monitored in accordance with the framework?

Defence has not consistently complied with the requirements of its assessment and authorisation process. For example, for all five systems examined:

- key supporting data had not been entered into Defence's ICT authorisation management system, and mandatory security documentation had not been provided to the Security Assessors;
- Defence was unable to substantiate that document reviews and control implementation assessments took place as required; and
- there were shortcomings in the peer review process, including not identifying that mandatory security documentation was missing, and not identifying inaccuracies and errors in Risk Assessments.

There were instances where systems had been re-authorised based on the re-authorisation triggers in the DSPF. These re-authorisations were not always granted prior to authorisation expiry.

3.74 Defence's policy and procedural requirements for ICT system authorisation are set out in the DSPF and Defence's assessment and authorisation process. To examine Defence's application of relevant requirements, the ANAO selected five Defence ICT systems for case study analysis. These systems were selected from the Defence ICT inventory project list. One system was selected from each Service (Army, Navy, and Air Force), Defence's Joint Capabilities Group (JCG) and the Chief Information Officer Group (CIOG), based on the highest recorded procurement cost[115] and the most recently completed authorisation process.[116] The five systems selected by the ANAO are outlined in Table 3.3.

3.75 For the each of the five systems in Table 3.3, ANAO reviewed Defence's most recent authorisation process for that system against relevant requirements of the July 2020 DSPF Principle 23 and Control 23.1 and the four steps of Defence's assessment and authorisation process: lodge

115 The procurement cost of systems is recorded within a range in Defence's ICT inventory system. The procurement cost ranges are: $0 – $1,000; $1,000 – $50,000; $50,000 – $500,000; $500,000 – $1 million; $1 million – $10 million; $10 million – $100 million; and $100 million – $500 million.

116 These systems were selected after excluding systems that did not have: an authorisation status recorded as 'Active'; an 'Environment type' recorded as 'Production'; and a 'Lifecycle' recorded as 'Active'.

certification and accreditation request; conduct certification assessment; review certification assessment; and finalise certification and accreditation.

Table 3.3: Case study summary

Case study	Authorisation date	Procurement cost $	Residual risk
Army case study[a]	14 June 2022	1000 – 50,000	Low
Navy case study	20 October 2021	50,000 – 500,000	Moderate
Joint Capabilities Group case study	1 November 2021	1m – 10m	Low
Air Force case study	1 November 2022	1m – 10m	Low
Chief Information Officer Group case study	5 December 2022	10m – 100m	Low[b]

Note a: This system was assigned to Army in the Defence ICT inventory list. However, the system has multiple versions that operate across different Services and Groups, including Army, Navy, and Air Force. Defence advised the ANAO in February 2024 that the relevant task for this system in Defence's ICT authorisation management system 'superseded the individual Service and Joint Operations Command implementations of … a capability-level accreditation'. ANAO review of this case study is limited to the system used by Army (see Army Case Study).

Note b: This system was allocated a residual risk rating of 'Low' in the Defence ICT inventory list. The Decision Brief for this system notes a residual risk of 'Moderate'. The same brief also notes in the overall assessment that, 'Based on its inherent risk and implemented controls, ICTSB [now DCIAB] has assessed the residual risk of the system to be LOW.'

Source: ANAO analysis.

Lodge certification and accreditation request

3.76 As discussed at paragraphs 2.56–2.57, Defence's assessment and authorisation process states that the lodgement of a request for system authorisation is done by the System Owner or their delegate through Defence's ICT intranet job portal. The process also requires System Owners to: provide detailed information to support the authorisation process, including entering system data (such as design information, threats and risks, and details of relevant personnel and business units) into Defence's ICT authorisation management system; conduct a Business Impact Level (BIL) assessment; and provide a System Risk Score document and a System Security Plan (SSP).

3.77 The five selected systems were assessed against these requirements and the results are outlined in Table 3.4.

Table 3.4: Lodgement of supporting information with ICT assessment and authorisation requests

Case study	Authorisation management system data	BIL assessment	System Risk Score document	System Security Plan
Army case study	◑	◑	○	○
Navy case study	◑	○	◑	○
Joint Capabilities Group case study	◑	○	○	○

Case study	Authorisation management system data	BIL assessment	System Risk Score document	System Security Plan
Air Force case study	◑	●	○	○
Chief Information Officer Group case study	◑	●	◑	◑
Key: ○ Not met ◑ Partly met ● Fully met				

Source: ANAO analysis of Defence documents.

3.78 Defence did not consistently apply its assessment and authorisation process in the following respects.

- For all five systems examined, complete data had not been entered in Defence's ICT authorisation management system, despite this information often being available in supporting security documents.
- For two systems, a BIL assessment had not been conducted. For one further system, a BIL rating had been assigned in supporting documentation, but the basis for this rating was not documented in a BIL assessment.
- For three systems, a System Risk Score document was not completed.[117] For the two remaining systems, the system characteristics and controls sections of the Security Risk Score document had been completed, but the responses had not been assessed or scored by DCIAB.[118] In one of the documents not assessed by DCIAB, the System Owner had not assessed their system as being compliant with the 'ASD Top 4'.[119]
- For four systems, the correct SSP template had not been completed. For these systems, alternative documentation was submitted instead, including Standard Operating Procedures (SOPs)[120], unsigned System Overview Documents, and a custom SSP.[121] For the

117 One of these systems was the Army case study. In a briefing to the system's Executive Board in July 2019, DCIAB stated that the System Risk Score document met 'the practical intent of an SRMP [System Risk Management Plan]', and that the requirement to provide a System Risk Score document had 'been superseded by the need for a full SRMP for each system'. The System Risk Score documentation and the SRMP are separate documents, each with their own template. As noted at footnote 48 and paragraph 2.62, Defence intranet guidance states that the System Risk Score document was replaced with a System Security Plan (SSP) Essential Eight Annex from 1 January 2023 and that the SRMP is an optional document that 'may be required depending on the nature and complexity of the system'.

118 As discussed at paragraph 2.58, the System Risk Score document enables DCIAB to assess the overall system risk and allocate a risk score, based on the System Owner's assessment of the Business Impact Level, system characteristics and potential security management controls.

119 As discussed at paragraph 1.7, PSPF Policy 10 requires entities to mitigate common security threats by implementing eight essential mitigation strategies (the Essential Eight). Prior to February 2022, only four of the strategies were mandatory (the 'ASD Top 4'). The System Risk Score document used to complete the assessment was unsigned and undated, and was based on a template with an 'effective date' of 21 October 2013.

120 The SOPs did not follow the DCIAB SOP template, and instead provided an overview of the system design and security controls.

121 Key elements of the SSP template involve assessing system compliance against the ISM and outlining arrangements for ongoing system monitoring. For the three systems that utilised SOPs or a System Overview Document in place of a SSP, the documents did not include those key elements of the SSP template.

one system where the correct SSP template had been completed, the SSP had not received executive sign-off and approval as required by the template.

Army case study

The system examined for this case study is a workforce management and activity planning system. Defence operates multiple instances of the system, including separate versions for Army, Navy and Air Force. As outlined in Table 3.3, this case study was selected on the basis of its allocation to Army and therefore only considers authorisation of the Army instance of the system.[a]

In July 2016, a vulnerability assessment was conducted in response to a security incident identified in December 2015 involving the inappropriate use of an administrative user account. The assessment identified security deficiencies and concluded that the system presented an 'Extreme risk to Defence information'.[b]

In February 2017, the Army and Air Force instances of the system were jointly assessed for re-authorisation. The Risk Assessment noted the 2016 vulnerability assessment and the development of a Security Remediation Plan[c] and identified that 'some initial remediation has already been undertaken'.[d]

In the Risk Assessment, DCIAB assessed the residual risk of the system as 'High' and concluded that 'the system would not present any additional risk to the Defence Single Information Environment'.[e] The Risk Assessment proposed additional security controls, including: implementation of the Security Remediation Plan; an additional vulnerability assessment to validate the implementation and effectiveness of controls identified in the Security Remediation Plan; the development of a Security Risk Management Plan, System Security Plan, and Standard Operating Procedures; and completion of a System Risk Score document.[f] The additional vulnerability assessment was not conducted, and the System Security Plan and Standard Operating Procedures were not developed.

The system was granted a 12-month provisional authorisation in March 2017 to allow for additional security controls to be implemented.

In October 2018, a Risk Assessment was signed off to support re-authorisation of the system, following expiry of the provisional authorisation in March 2018. The Risk Assessment stated that the system assessment was based on a Vulnerability Assessment and System Risk Score document. The vulnerability assessment and System Risk Score document were both dated July 2016.

The Risk Assessment also outlined controls implemented to reduce risk. While none of these were new controls as they had all been referenced in the 2017 Risk Assessment, the system's risk rating was reduced to 'Moderate', down from 'High' in the previous Risk Assessment.[g] The Risk Assessment did not include an assessment of the implementation of recommendations from the 2016 vulnerability assessment, System Remediation Plan, or conditions issued under the previous authorisation.[h] The system was granted a three-year authorisation in December 2018.

A Risk Assessment, approved in June 2022 in order to obtain re-authorisation for the system, noted that the system assessment was based on a System Overview Document (SOD) and

Security Risk Management Plan (SRMP). The SRMP uploaded to Defence's ICT authorisation management system is an unapproved document with a recorded release date of August 2019.[i] The SOD was not uploaded to the authorisation management system.[j] The system's residual risk was assessed as 'Low' and a three-year authorisation was granted on 14 June 2022.

Note a: The Army system was initially introduced and authorised for use by Navy in December 2008. As part of an upgrade, system functionality was extended for use by Army in January 2011. Historical documentation for this system indicates that the system was granted authorisations in January 2011, July 2013 and September 2013. Subsequent authorisations are discussed in the Army case study.

Note b: Deficiencies identified included poor password security, sharing of administrator credentials, and uncontrolled changes being made to the system. The vulnerability assessment also noted that 'it is likely that the findings included in this report relate to all [system] environments'.

Note c: The Security Remediation Plan was released in November 2016 and outlined actions to be taken including: implementing policies and procedures for logging and monitoring in line with ISM requirements; resetting of account passwords and disabling of shared accounts; updating documentation to reflect current system configuration; and implementation of a change management process.

Note d: The Risk Assessment did not detail what specific remediation action had been undertaken from the Security Remediation Plan.

Note e: Conversely, it was stated elsewhere in the Risk Assessment that 'ICTSB has assessed that the current implementation [of the system and controls] does not address security concerns identified during the development and certification process and does not meet the requirements for effective security.'

Note f: The heightened risks for this system were reflected in a July 2016 System Risk Score document for the Army and Air Force instances of the system. All 11 'potential security management controls' listed as part of the System Risk Score template were identified as applicable to and selected for implementation for the system (including an annual review of the Security Risk Management Plan, and vulnerability assessments/scans conducted on a sample basis at least every two years).

A risk score of 'Excellent' was allocated to the system in the July 2016 System Risk Score document, despite many controls being assessed as either not applicable or not implemented. DCIAB referenced the 2016 Vulnerability Assessment when documenting the basis for this score in the System Risk Score document but did not address how it had arrived at a result that differed from the Extreme risk in the Vulnerability Assessment. DCIAB noted that the System Risk Score document would not be used for the assessment and authorisation process, instead relying on the Vulnerability Assessment.

Note g: One control had been amended to note that server infrastructure previously managed by CIOG had been transitioned to an IT company, Leidos.

Note h: Minutes from a meeting of the system's Executive Board in May 2018 stated that 'A security assessment and certification is currently underway by ICTSB [now DCIAB] and is expected to conclude in early June 2018. The review will determine if all 2016 recommendations have been remediated'.

Note i: A briefing to the system's Executive Board in July 2019 noted that DCIAB recommended the creation of an SRMP for each instance of the system. The single SRMP uploaded to Defence's ICT authorisation management system refers to the Army, Navy and Air Force instances of the system.

Note j: A SOD for the Navy instance of the system was filed in Defence's electronic document and records management system, Objective, and was last reviewed in June 2016. Defence advised the ANAO in June 2024 that the SOD for the Navy instance was used as the basis for the whole-of-Defence implementation of the system as the Navy instance represented 'the greatest complexity due to its needs to operate in a disconnected state while offshore.'

Conduct certification assessment

3.79 As discussed at paragraph 2.66, once the security documentation is submitted by the System Owner, it is reviewed by the Security Assessor (Certification Consultant) 'for accuracy, completeness, and to ensure sufficient information is provided to carry out the assessment'.[122] Once the Security Assessor has all required information, a 'Stage 1 Assessment' is conducted, which includes: a detailed analysis of the system design to assess risks; a determination as to whether

122 DSPF Control 23.1 requires that Security Assessors are 'formally appointed (in writing) by a Certification Authority (CA) or delegated representative'. Defence was unable to provide evidence that the Security Assessors were formally appointed for any of the five case studies.

appropriate security controls have been implemented; and a review of all relevant controls specified in the ISM and DSPF.

3.80 The five selected systems were assessed against these requirements and the results are outlined in Table 3.5.

Table 3.5: Conduct of certification assessments

Case study	Review of documentation	Analysis of system design	Determination of control implementation	Review of ISM and DSPF controls
Army case study	○	◑	◑	○
Navy case study	○	◑	◑	◑
Joint Capabilities Group case study	○	◑	◑	○
Air Force case study	○	◑	◑	◑
Chief Information Officer Group case study	○	●	◑	◑
Key: ○ Not met ◑ Partly met ● Fully met				

Source: ANAO analysis of Defence documents.

3.81 Defence did not consistently apply its assessment and authorisation process in the following respects.

- As noted in Table 3.4, at least some of the mandatory security documents to support system authorisation were missing for all five systems. This was not addressed prior to the system authorisation process commencing. There was no evidence of the Certification Consultant reviewing the sufficiency of documentation or requesting missing documentation from the System Owner for the five case studies.[123]
- For four systems, deficiencies were identified in the analysis of system design, including:
  - one system where no system-specific risks had been identified either in supporting security documentation, or as part of the assessment process[124];

123 Defence advised the ANAO in June 2024 that:

> An assessment would not have been completed in the case where a Certification Consultant had insufficient information. Coverage within the supplied documentation was considered sufficient to inform the establishment of inherent risk and an assessment of residual risk.

124 While there was no risk information provided to inform an assessment, the system was allocated an overall residual risk rating following DCIAB's analysis of the documentation. The Risk Assessment for this system stated that the residual risk was determined based on an assessment of the system's 'capabilities, inherent risk and implemented controls'. Step 2 of the ISM six-step process (see Figure 1.1) requires entities to 'identify the security risks to each ICT system and select fit-for-purpose security controls that are proportionate to the security risks identified and consistent with the entity's agreed risk tolerances.'

  - two systems where the supporting security documentation identified connections to unauthorised systems. Neither the system documentation nor the assessment process outlined the risks associated with these connections[125]; and
  - one system where the assessment was based on out-of-date documentation (see Army Case Study).
- For all five systems, there were deficiencies in Defence's review of ISM and DSPF controls. There was no evidence that DSPF controls were reviewed across the five systems, and there was no evidence that ISM controls were reviewed across two systems.[126]

3.82 For all five systems examined, the Risk Assessments included statements by DCIAB that the system security assessment was based on an assessment of 'current system implementation'. Defence was unable to provide evidence that system security controls for each case study were assessed as to whether they had been correctly implemented and operating as intended, as required under Step 4 of the ISM six-step process.

Navy case study

The Navy case study system supports Navy's capabilities and was delivered to Navy in January 2021.

The system was allocated with a three-month provisional authorisation on 27 January 2021, as DCIAB's security assessment identified that the 'system implementation does not address security concerns for a system of its type and data sensitivity.' The authorisation package proposed the implementation of additional controls during the provisional authorisation period, to be assessed as part of system re-authorisation, including:

- the development of a 'mature security document suite exhaustively detailing the implementation, operation, management and sustainment of [the system]', submitted in accordance with Defence templates; and
- an assessment of all applicable ISM controls, in accordance with the SSP Annex.

A request for re-authorisation was lodged in Defence's ICT authorisation management system in May 2021 and included an unassessed System Risk Score document and a 'Standard Operating Procedures' (SOPs) document. The SOPs did not outline standard operating

125 PSPF Policy 11 states that 'Interconnection of ICT systems creates a potential vector for adversaries to target the system via third parties. As part of the security assessment and authorisation process, where an ICT system will be connected to other systems outside the entity's control, consider the security risks and what security protections are required between the systems'.
- The SSP for the Air Force case study stated that 'Limited documentation has been provided from the Chief Information Officer Group (CIOG) regarding the connected systems of [the case study system]; therefore, the security posture of connected systems for the purpose of certification and accreditation (C&A) activities is considered to be unknown.'
- The Risk Assessment for the Joint Capabilities Group case study identified that a key risk for the system related to an outsourced firewall and security monitoring service utilised by the system. The Risk Assessment stated that 'There is no overarching accreditation or endorsement through ICT Architecture Branch for [the outsourced system] to host, store, process and/or communicate Defence information. As such, there is no formal risk assessment of [the outsourced system], nor is there any formal risk acceptance for Defence systems to be hosted on [the outsourced system]'.

126 For two of the five systems, the incomplete System Risk Score documents indicated that the systems were 'compliant with any relevant/specific security controls within the ISM/PSPF/DSPF'.

procedures for the system (as required by the SOP template). Rather, it provided a system overview, including outlining controls implemented in relation to system security. A BIL and SSP were not submitted for this system. These documents are required under Defence's assessment and authorisation process and formed part of the 'mature security document suite' listed as a condition of the three-month provisional authorisation.

The Decision Brief and Risk Assessment for the re-authorisation request were provided to the Assessment Authority and Authorising Officer in October 2021. The Decision Brief outlined the 'impact to operations if the [system] is not Accredited', noting that the system had been granted a Provisional ICT Accreditation (PICTA) and was a critical element of Navy's capability. The Decision Brief also noted that:

> In the PICTA, it was recommended to provide mature security documents, apply hardening guide on Windows10 operating system and use secured data transfer devices. The [system] has now fulfilled all PICTA recommendations.

This statement was incorrect, as a complete security document suite had not been provided. The Authorising Officer signed the Decision Brief on 20 October 2021, issuing the system with a three-year authorisation.

Review certification assessment and finalise accreditation

3.83 As discussed at paragraphs 2.69–2.71, Defence's process requires that the drafted Risk Assessment is reviewed by a peer reviewer, agreed to by the System Owner, and then signed by the Security Assessor and endorsed by the Assistant Director or Director of DCIAB's Integrated Risk Management (IRM) directorate (now the Directorate of Cyber Security Assessment and Authorisation). The Decision Brief (which includes the approved Risk Assessment) then proceeds to the Assessment Authority and Authorising Officer for approval.

3.84 The five selected systems were assessed against these requirements and the results are outlined in Table 3.6.

Table 3.6: Implementation of assessment and authorisation

Case study	Peer review	System Owner acceptance	Risk Assessment signed	Assessment Authority approval	Authorising Officer approval
Army case study	◑	●	●	●	●
Navy case study	◑	●	◑	●	● [a]
Joint Capabilities Group case study	◑	●	●	●	●
Air Force case study	◑	●	●	●	●
Chief Information Officer Group case study	◑	●	●	●	●
Key: ○ Not met ◑ Partly met ● Fully met					

Note a: The Authorising Officer for this system was the Director General Navy Intelligence and Information Warfare (DGNIW), however, the system was allocated to the Capability Acquisition and Sustainment Group (CASG) in

Defence's ICT authorisation management system. Defence advised the ANAO in June 2024 that the allocation of the system to CASG in the authorisation management system was an error.

Source: ANAO analysis of Defence documents.

3.85 There was evidence that the assigned peer reviewer reviewed the Risk Assessments for all of the case studies. Those peer review processes did not identify:

- that key required documents were missing for each of the case study systems[127];
- inaccuracies in Risk Assessments for three systems, including:
  - a statement in the Risk Assessment for the Navy system that the system had 'fulfilled all PICTA recommendations', despite some conditions of the provisional authorisation not being met (see Navy case study);
  - conflicting statements in the Risk Assessment for the Joint Capabilities Group system, which stated that DCIAB 'has no additional security proposals' for the system while the subsequent paragraph, referring to the same assessment and authorisation process, stated that DCIAB had 'recommended controls … for maintaining the current security posture'; and
  - conflicting residual risk ratings in the Risk Assessment for the Chief Information Officer Group system (see Table 3.3, Note b); and
- deficiencies in the Risk Assessment for the Air Force system, which did not identify that the system had previously been granted provisional authorisation and did not outline whether the conditions of the provisional authorisation had been addressed (see Air Force case study).

3.86 For all five systems, Defence had documented the System Owner's (or their delegate's) acceptance of the proposed authorisation recommendations and the Risk Assessment was signed by the Security Assessor.[128] For all five systems, the Decision Brief was signed by the relevant Assessment Authority and Authorising Officer as outlined in the DSPF.[129]

Operational impact of system authorisations

3.87 For four systems, the Decision Briefs outlined the 'impact to operations' if the systems were not authorised. For one of these systems (see Air Force case study), the assessed residual risk and authorisation decision changed over a three-month period, following the identification of operational impacts.

3.88 PSPF Policy 11 requires that the CSO or CISO 'checks that due consideration has been paid to risk, security, functionality and business requirements' as part of the assessment process. A variation of this requirement is outlined for Authorising Officers. The policy requires Authorising

127 The Risk Assessment for each system outlined the documentation that was used as the basis for the security assessment, however they did not address why mandatory documentation was missing and the impact that this had on the assessment process.

128 For the Navy system, which had a residual risk rating of 'Moderate', the Risk Assessment was subsequently endorsed by the Assistant Director Certification Management (an EL1 official). Defence's ICT authorisation management system SOPs state that systems with a risk rating above 'Low' are to be submitted to the Director of Integrated Risk Management (an EL2 official) for endorsement.

129 For the Air Force system, the Decision Brief was only signed off by the Head of ICT Operations (HICTO) as the Authorising Officer. Previous authorisations for this system had been provided jointly by the HICTO, Chief of Joint Operations, and CISO (see Air Force case study, Note g).

Officers to authorise systems to operate 'based on the acceptance of the security risks associated with its operation' (see Figure 1.1).

3.89 While the inclusion of operational impacts in the briefs may provide important context for the Authorising Officer, there is no evidence regarding the extent to which operational impacts have been factored into the decision for authorisation for the four systems.

Opportunity for improvement

3.90 There is an opportunity for Defence to improve its documentation to clarify the extent to which operational impacts have been factored into the decision to authorise systems.

System monitoring

3.91 As discussed at paragraph 3.4, the DSPF establishes the responsibility for System Owners to obtain and maintain authorisation of their systems and requires ICT systems to be re-authorised when one or more of the conditions outlined in Box 1 are met.

Box 1: Triggers for system re-authorisation

- Commonwealth or Defence policy changes;
- New or emerging threats to systems are detected;
- Security measures are not operating as effectively as planned;
- A cyber security incident occurs;
- Changes to the certified system architecture occur;
- Changes to the system risk profile occur;
- The system extends outside the accreditation boundary;
- The physical environment in which the system is installed changes; or
- The system's accreditation expires.

Note: Defence's Assessment and Authorisation Framework, released in May 2024, includes an additional re-authorisation trigger: 'actions identified in a system's Remediation Plan are not implemented'. DSPF Control 23.1, updated in May 2024, states that 'systems are Re-Assessed and Re-Authorised throughout the system's lifecycle in line with re-assessment triggers and timeframes set by the Authorising Delegate'.

Source: Defence Security Principles Framework.

Re-authorisation due to authorisation expiry

3.92 Of the five systems examined, four have undergone multiple authorisation processes due to authorisation expiry. ANAO reviewed these four systems to assess whether re-authorisation was sought upon authorisation expiry, and found that there were gaps in the authorisation periods for some systems as follows:

- authorisation for the Army system expired on 30 March 2018, but the system was not re-authorised until 11 December 2018 (see Army case study);

- authorisation for the Navy system expired on 26 April 2021, but the system was not re-authorised until 20 October 2021 (see Navy case study)[130]; and
- authorisation for the Air Force system expired on 6 November 2020, but the request for re-authorisation was not submitted until April 2021, and the system was not re-authorised until 1 November 2022 (see Air Force case study).

3.93 These systems remained operational during the period their authorisations had lapsed.

3.94 A system operating under four consecutive provisional authorisations between January 2018 and September 2020 is discussed in the Air Force case study.[131]

Air Force case study

The Air Force system supports data exchange between Air Force and other Defence systems. The system was deployed into a production environment in March 2018.

Three provisional authorisations were granted for this system between January 2018 and June 2018.

A Decision Brief provided in January 2018 outlined three authorisation options and their associated levels of assessed residual risk:

- Option 1 — deny accreditation to the whole system (no residual risk);
- Option 2 — provisionally authorise lower risk components of the system and deny accreditation to the higher risk component (moderate risk); or
- Option 3 — provisionally accredit the full system (significant risk).[a]

DCIAB recommended Option 2 as there was no evidence of certification of the higher risk component and insufficient information about its security and connections to other systems.[b] The Authorising Officer supported a 12-month provisional authorisation under Option 2 on 6 February 2018.

A subsequent Decision Brief in March 2018 provided the same three options but included a new section titled 'business context', which outlined the operational impact of not authorising the full system, including the higher risk component.

The brief noted that the business area had 'made changes to the system to strengthen data protection mechanisms and increasing [sic] CIOG oversight of the system'. Following assessment, the residual risk rating of Option 3 had been reduced from 'significant' to 'moderate' (the same risk level as the more limited Option 2). The basis for this reduction was not clear, as DCIAB's assessment identified that the evidence of certification of the higher risk component had still not been provided.[c] The overall residual risk of the system was still assessed as 'Significant'.[d] The full system was granted a second 12-month provisional authorisation on 15 March 2018.

130 Defence advised the ANAO in June 2024 that the re-authorisation request for this system was entered into Defence's ICT authorisation management system in May 2021.

131 A similar observation was made in Auditor-General Report No.24, 2022–23, *Defence's Management of the Delivery of Health Services to the Australian Defence Force,* which found that the full authorisation of a Defence contractor ICT system 'was not completed in a timely manner' as the system operated under a provisional authorisation for almost four years (see paragraph 4.19 of that audit).

A further Decision Brief was submitted in May 2018, as a result of system changes. DCIAB assessed the residual risk as 'Significant' and a third 12-month provisional authorisation was granted on 6 June 2018, to allow for the implementation of additional controls including improving the security document suite and the conduct of a 'Stage 2 Audit'.

In September 2019, a new Decision Brief was submitted, following the expiry of the previous provisional authorisation. DCIAB assessed the residual risk as 'Moderate' and noted that a 'Stage 2 assessment is required to determine whether the security controls are implemented and are operating effectively.'[e] The brief also noted that the system risk could not be reduced below 'Moderate' until a Stage 2 assessment had been conducted, and proposed the implementation of additional security controls, including improvements to supporting security documentation. Completion of the 'Stage 2 assessment' and improved security documentation were also required under the conditions of the previously issued provisional authorisation.

Defence advised the ANAO in June 2024 that a Stage 2 assessment was not conducted. Defence further advised that the requirement to conduct the assessment was captured in an earlier system for managing system authorisations (see footnote 87), but was not included in the migration of data to Defence's ICT authorisation management system, and that, as a result, the 'Certification Consultant assigned to the subsequent … task was unaware of this recommendation when completing their assessment.'

The September 2019 Risk Assessment and Decision Brief did not outline whether issues raised in previous provisional authorisations had been addressed. The system was granted a fourth 12-month provisional authorisation in November 2019.

A request for re-authorisation was submitted in April 2021. Despite required improvements to security documentation being noted as a condition of the previous two provisional authorisations, a mandated System Risk Score document was not provided to support authorisation. The Risk Assessment did not outline whether the conditions of previous provisional authorisations had been addressed.[f] DCIAB assessed the residual risk of the system as 'Low', and a three-year authorisation was granted on 1 November 2022.[g] The assessment of the residual risk as 'Low' was not consistent with the previous authorisation process which found that the system risk could not be reduced below 'Moderate' until a Stage 2 assessment had been conducted.

Note a: A subsequent paragraph in the Decision Brief rated this option as having an 'Extreme' risk.

Note b: The Risk Assessment which accompanied the Decision Brief identified the primary sources of system risk including insufficient detail regarding security controls in security documentation and vulnerabilities identified through a vulnerability assessment that required remediation.

Note c: Further, DCIAB had noted that work to address some of the primary sources of system risk identified in the original Risk Assessment (see Note b) had not been finalised.

Note d: The brief stated that 'The Commander of Air Combat Group [CACG] is responsible for the acceptance of risks relating to the compromise of sovereign data from this system. Whilst controls identified … will contribute to managing these risks, they are interim measures … CACG will provide a brief to HICTO formally accepting this risk.' CACG approved a brief in December 2019 accepting an assessed risk of 'Moderate'. Defence advised the ANAO in August 2024 that it was 'unable to identify evidence that this brief was provided to HICTO.'

Note e: The ISM six-step process requires an assessment of control implementation to be done before granting authorisation (see Figure 1.1).

Note f: The May 2020 internal audit report into *Certification and Accreditation of Defence ICT Networks* found that there was 'limited management and oversight where a Provisional ICT Accreditation (PICTA) had been issued, presenting a risk that networks and systems continue to operate where they have been deemed too high-risk to achieve full accreditation'.

DCIAB conducted a review of the draft Risk Assessment in July 2021, suggesting minor editorial amendments. However, further feedback from DCIAB in November 2021 noted that 'the [Risk Assessment] was difficult to read' and suggested further changes, including providing more detail on the nature of the system. Further feedback from DCIAB in April 2022 included similar comments. A final revised Risk Assessment was submitted in October 2022.

Note g: The May 2018 and September 2019 Decision Briefs identified that the system required authorisation from three Authorising Officers due to 'system connectivity and information ownership'. These officers were HICTO, the Chief of Joint Operations, and the CISO. At the time of these authorisations, the CISO and the Assistant Secretary ICT Services Branch (who is the Assessment (Certification) Authority for Defence systems under the DSPF), were different officers. The November 2022 Decision Brief was only signed off by the HICTO. Defence advised the ANAO in June 2024 that '[f]ollowing transfer of the CISO role to Assistant Secretary ICT Security Branch, that position already had complete visibility of system authorisations as the Certification Authority, and the extra authority was not required'. Defence did not provide an explanation for why authorisation was no longer required from the Chief of Joint Operations.

Re-authorisation due to Commonwealth or Defence policy changes

3.95 As noted in paragraphs 1.7–1.10, PSPF Policy 10 and 11 were updated in February 2022 and August 2020 respectively. Notable policy changes prior to this include the initial release of PSPF Policy 10 and 11 in September 2018. Under the DSPF, these changes are triggers for re-authorisation (see Box 1).

3.96 Of the five systems examined by ANAO: two systems were operational when the revised PSPF was introduced in September 2018 and when PSPF Policy 11 was updated in August 2020; and four systems were operational when PSPF Policy 10 was updated in February 2022. The documentation for these systems did not identify any references to the PSPF updates.

Re-authorisation due to system changes

3.97 Across the five case studies, there were three instances where re-authorisation had been sought with reference to system changes:

- a Decision Brief was approved in June 2018 for the Air Force system noting that 'the system functionality has been extended';
- the Army system was re-authorised in January 2011 due to the system being extended for use by Army; and
- the Army system was re-authorised in July 2013 due to changes to the system's operating location.

Recommendation no. 8

3.98 The Department of Defence implements arrangements to ensure that PSPF requirements, DSPF requirements and Defence's assessment and authorisation process are complied with, including:

(a) ensuring that all required documentation has been completed prior to system assessment and authorisation;

(b) documenting the approval and review of mandatory supporting documentation;

(c) conducting and documenting assessments of the implementation and effectiveness of controls and provisional authorisation conditions against all relevant ISM and DSPF controls; and

(d) ensuring systems are proactively monitored against the conditions for re-authorisation.

Department of Defence response: *Agreed.*

3.99 *The current Cyber Policy Hub will be augmented as part of the A&A [Assessment and Authorisation] Improvement Program to ensure the regular scanning and updates of key related government policies impacting cyber security ICT authorisation. These policies will be assessed and reflected in the department's policies, frameworks, practices and processes.*

3.100 *The Cyber Policy Hub will also be responsible for implementing and enforcing first and second level assurance over the A&A framework, DSPF principle 23 and 23.1 controls. This will ensure compliance at all levels of obligation, including evaluating control effectiveness, managing provisional authorisations, and overseeing re-authorisations, in addition to meeting minimum compliance requirements.*

Rona Mellor PSM
Acting Auditor-General

Canberra ACT
11 September 2024

Appendices

Appendix 1 Department of Defence response

Australian Government
Defence
PO Box 7900 CANBERRA BC ACT 2610

EC24-003873

Ms Rona Mellor, PSM
Acting Auditor-General
PO BOX 707
CANBERRA ACT 2601

Dear Ms Mellor

Auditor-General Proposed Report – Defence's management of ICT security authorisations

Thank you for the opportunity to comment on the Proposed Report for the Auditor-General performance audit *Defence's management of ICT security authorisations.*

Defence acknowledges and accepts the key findings, recommendations and the opportunity for improvement, which are aimed at improving Defence's Cyber Security Assessment and Authorisation Framework. Defence is committed to strengthening our approach to safeguard data from cyber threats and ensuring the secure operation of ICT systems to protect the continuous delivery of Defence outcomes and capabilities.

Attached to this letter are Defence's proposed amendments, editorials and comments (**Annex A**), response to requests for information (**Annex B**), response to proposed recommendations (**Annex C**) and Defence's summary response (**Annex D**). These constitute Defence's formal response to the Auditor-General Proposed Report.

Our point of contact is the ANAO Liaison Officer who can be contacted via email at: anao.lo@defence.gov.au.

Yours sincerely

Matt Yannopoulos PSM
Acting Secretary

7 August 2024

Robert Chipman, AO, CSC
Air Marshal
Acting Chief of the Defence Force

7 August 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 appropriately implemented.

- As noted at paragraph 2.6, Defence Security Principles Framework (DSPF) Principle 23 and Control 23.1 were approved by the Chief Information Security Officer on 10 May 2024.
- As noted at paragraph 2.9, the Chief Information Security Officer has been appointed as the Control Owner in the May 2024 DSPF Control 23.1.
- As noted at footnote 65, Defence advised the ANAO in April 2024 that the Army ICT Security Plan directive had been updated and was awaiting delegate approval.
- As noted in paragraph 2.38, a new version of Air Force instruction AFSI (OPS) 05-02 was published in June 2024 and requires all Air Force ICT systems to be authorised prior to operation.
- As noted at footnote 42, in March 2024, Air Force's 462 Squadron (which is responsible for system assessment activities within Air Force) transitioned to the Joint Capabilities Group.
- As noted at paragraph 2.50, in February and May 2024, the Defence Chief Information Security Officer approved and released the Assessment and Authorisation Framework.
- As noted at footnote 76, Defence advised the ANAO in January 2024 that it had decided to revisit the need to request reporting from the Defence Finance Group to identify systems which have not been authorised.

- As noted at footnote 82, Defence advised the ANAO in June 2024 that the ICT inventory project 'is due to be finalised for system owners to access and update their information by mid-July 2024. The team will work to transition the [inventory system] into sustainment by November 2024'.
- As noted at paragraph 3.56, the DSPF was updated in March 2024 to reflect changes to the frequency of Control Owner reporting to the Defence Security Committee.
- As noted at paragraph 3.61, in May 2024, Defence commenced providing Control Owner reports directly to the Defence Security Committee, in accordance with the requirements of the Defence Security Principles Framework (DSPF). The report provided to the Defence Security Committee in May 2024 included information not available in previous reports, outlining deficiencies in relation to Control 23.1, including that: assessment and authorisation policy was not current; Defence's ICT authorisation management system did not sufficiently support an enterprise-wide view of ICT risks; and the volume of Defence ICT systems outweighs available resources for assessment and authorisation activities.

Appendix 3 System accreditation status by residual risk rating

Accreditation status	Risk rating	Proportion of systems (%)
No accreditation	Unknown	14.73
	Extreme	0.04
	Significant	0.34
	High	0.21
	Moderate	2.72
	Low	2.85
	Blank	0.04
	Total	**20.93**
Active	Unknown	0
	Extreme	0
	Significant	0.47
	High	0.04
	Moderate	5.28
	Low	5.87
	Blank	0
	Total	**11.66**
New in progress	Unknown	21.63
	Extreme	0
	Significant	0.09
	High	0.26
	Moderate	1.62
	Low	2.85
	Blank	0.09
	Total	**26.54**
In re-accreditation	Unknown	0.21
	Extreme	0
	Significant	0.81
	High	0.34
	Moderate	6.98
	Low	6.05
	Blank	0
	Total	**14.39**

Expired	Unknown	0.35
	Extreme	0.04
	Significant	1.58
	High	1.49
	Moderate	9.58
	Low	13.45
	Blank	0
	Total	**26.49**

Source: ANAO analysis of Defence's ICT authorisation management system.