



Information security manual

Guidelines for cyber security documentation

Last updated: September 2026

Development and maintenance of cyber security documentation

Cyber security strategy

A cyber security strategy articulates an organisation's vision, guiding principles, objectives and priorities for cyber security, typically over a five-year period. In addition, a cyber security strategy may also cover an organisation's threat environment, cyber security initiatives or investments the organisation plans to make as part of its cyber security program. Without a cyber security strategy, an organisation risks failing to adequately plan for and manage security and business risks within their organisation.

Control: ISM-0039; **Revision:** 6; **Updated:** Dec-22; **Applicable:** NC, OS, P, S, TS; **Essential 8:** N/A

A cyber security strategy is developed, implemented and maintained.

Approval of cyber security documentation

If cyber security documentation is not reviewed and approved by an appropriate authority, system owners risk failing in their duty to ensure that appropriate security controls have been identified and implemented for systems and their operating environments. In doing so, it is important that a system's security architecture, as outlined within the system security plan and supported by the cyber security incident response plan, change and configuration management plan, and continuous monitoring plan, is approved by the system's authorising officer prior to the development of the system.

Control: ISM-0047; **Revision:** 6; **Updated:** Dec-25; **Applicable:** NC, OS, P, S, TS; **Essential 8:** N/A

Organisational-level cyber security documentation is approved by the chief information security officer while system-specific cyber security documentation is approved by the system's authorising officer.

Control: ISM-1739; **Revision:** 0; **Updated:** Mar-22; **Applicable:** NC, OS, P, S, TS; **Essential 8:** N/A

A system's security architecture is approved prior to the development of the system.

Maintenance of cyber security documentation

Threat environments are dynamic. If cyber security documentation is not kept up to date to reflect the current threat environment, policies, processes and procedures may cease to be effective. In such

situations, resources could be devoted to cyber security initiatives or investments that are less effective or no longer relevant.

Control: ISM-0888; Revision: 7; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A

Cyber security documentation is reviewed at least annually and includes a 'current as at [date]' or equivalent statement.

Communication of cyber security documentation

It is important that once cyber security documentation has been approved, it is published and communicated to all stakeholders. If cyber security documentation is not communicated to stakeholders, they will be unaware of what policies and procedures have been implemented for systems.

Control: ISM-1602; Revision: 2; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A

Cyber security documentation, including notification of subsequent changes, is communicated to all stakeholders.

Further information

Further information on system-specific cyber security documentation, such as a system security plan, cyber security incident response plan, change and configuration management plan, continuous monitoring plan, security assessment report and plan of action and milestones, can be found in the 'System-specific cyber security documentation' section of these guidelines.

Further information on system registers can be found in the 'Chief information security officer' section of the [Guidelines for cyber security roles](#).

Further information on business continuity and disaster recovery plans can be found in the 'Chief information security officer' section of the [Guidelines for cyber security roles](#).

Further information on cyber security communication strategies can be found in the 'Chief information security officer' section of the [Guidelines for cyber security roles](#).

Further information on cyber security incident management policy can be found in the 'Managing cyber security incidents' section of the [Guidelines for cyber security incidents](#).

Further information on cyber security incident registers can be found in the 'Managing cyber security incidents' section of the [Guidelines for cyber security incidents](#).

Further information on supplier relationship management policy can be found in the 'Cyber supply chain risk management' section of the [Guidelines for procurement and outsourcing](#).

Further information on approved supplier lists can be found in the 'Cyber supply chain risk management' section of the [Guidelines for procurement and outsourcing](#).

Further information on managed service registers can be found in the 'Managed services and cloud services' section of the [Guidelines for procurement and outsourcing](#).

Further information on outsourced cloud service registers can be found in the 'Managed services and cloud services' section of the [Guidelines for procurement and outsourcing](#).

Further information on authorised radio frequency and infrared device registers can be found in the 'Facilities and systems' section of the [Guidelines for physical security](#).

Further information on authorised medical device registers can be found in the 'Facilities and systems' section of the [*Guidelines for physical security*](#).

Further information on cyber security awareness training registers can be found in the 'Cyber security awareness training' section of the [*Guidelines for personnel security*](#).

Further information on general-purpose artificial intelligence usage policy can be found in the 'Cyber security awareness training' section of the [*Guidelines for personnel security*](#).

Further information on web usage policy can be found in the 'Cyber security awareness training' section of the [*Guidelines for personnel security*](#).

Further information on cable registers can be found in the 'Cabling infrastructure' section of the [*Guidelines for communications infrastructure*](#).

Further information on floor plan diagrams can be found in the 'Cabling infrastructure' section of the [*Guidelines for communications infrastructure*](#).

Further information on cable labelling processes and procedures can be found in the 'Cabling infrastructure' section of the [*Guidelines for communications infrastructure*](#).

Further information on telephone system usage policy can be found in the 'Telephone systems' section of the [*Guidelines for communications systems*](#).

Further information on denial of service response plans for video conferencing and Internet Protocol telephony services can be found in the 'Video conferencing and Internet Protocol telephony' section of the [*Guidelines for communications systems*](#).

Further information on multifunction device usage policy can be found in the 'Multifunction devices' section of the [*Guidelines for communications systems*](#).

Further information on mobile device management policy can be found in the 'Mobile device management' section of the [*Guidelines for enterprise mobility*](#).

Further information on mobile device usage policy can be found in the 'Mobile device usage' section of the [*Guidelines for enterprise mobility*](#).

Further information on mobile device emergency sanitisation processes and procedures can be found in the 'Mobile device usage' section of the [*Guidelines for enterprise mobility*](#).

Further information on information technology (IT) equipment management policy can be found in the 'IT equipment usage' section of the [*Guidelines for information technology equipment*](#).

Further information on networked and non-networked IT equipment registers can be found in the 'IT equipment usage' section of the [*Guidelines for information technology equipment*](#).

Further information on IT equipment sanitisation processes and procedures can be found in the 'IT equipment sanitisation and destruction' section of the [*Guidelines for information technology equipment*](#).

Further information on IT equipment destruction processes and procedures can be found in the 'IT equipment sanitisation and destruction' section of the [*Guidelines for information technology equipment*](#).

Further information on IT equipment disposal processes and procedures can be found in the 'IT equipment disposal' section of the [*Guidelines for information technology equipment*](#).

Further information on media management policy can be found in the 'Media usage' section of the [Guidelines for media](#).

Further information on removable media usage policy can be found in the 'Media usage' section of the [Guidelines for media](#).

Further information on removable media registers can be found in the 'Media usage' section of the [Guidelines for media](#).

Further information on media sanitisation processes and procedures can be found in the 'Media sanitisation' section of the [Guidelines for media](#).

Further information on media destruction processes and procedures can be found in the 'Media destruction' section of the [Guidelines for media](#).

Further information on media disposal processes and procedures can be found in the 'Media disposal' section of the [Guidelines for media](#).

Further information on system usage policy can be found in the 'Identity and access management' section of the [Guidelines for system access](#).

Further information on artificial intelligence agent registers can be found in the 'Identity and access management' section of the [Guidelines for system access](#).

Further information on system administration processes and procedures can be found in the 'System administration' section of the [Guidelines for system management](#).

Further information on patch management processes and procedures can be found in the 'System maintenance' section of the [Guidelines for system management](#).

Further information on software registers can be found in the 'System maintenance' section of the [Guidelines for system management](#).

Further information on digital preservation policy can be found in the 'Data backup and restoration' section of the [Guidelines for system management](#).

Further information on data backup processes and procedures can be found in the 'Data backup and restoration' section of the [Guidelines for system management](#).

Further information on data restoration processes and procedures can be found in the 'Data backup and restoration' section of the [Guidelines for system management](#).

Further information on security monitoring policy can be found in the 'Security monitoring' section of the [Guidelines for security assurance](#).

Further information on secure software development policy can be found in the 'Software development fundamentals' section of the [Guidelines for software development](#).

Further information on software developer cyber security knowledge and skills registers can be found in the 'Software development fundamentals' section of the [Guidelines for software development](#).

Further information on vulnerability disclosure policy can be found in the 'Software development fundamentals' section of the [Guidelines for software development](#).

Further information on vulnerability disclosure processes and procedures can be found in the 'Software development fundamentals' section of the [Guidelines for software development](#).

Further information on database registers can be found in the ‘Databases’ section of the [Guidelines for database systems](#).

Further information on email usage policy can be found in the ‘Email usage’ section of the [Guidelines for email](#).

Further information on network diagrams can be found in the ‘Network design and configuration’ section of the [Guidelines for networking](#).

Further information on cryptographic key management processes and procedures can be found in the ‘Cryptographic fundamentals’ section of the [Guidelines for cryptography](#).

Further information on data transfer processes and procedures can be found in the ‘Data transfers’ section of the [Guidelines for data transfers](#).

System-specific cyber security documentation

Context

System-specific cyber security documentation, such as a system security plan, cyber security incident response plan, change and configuration management plan, continuous monitoring plan, security assessment report, and plan of action and milestones, supports the accurate and consistent application of policies, processes and procedures for systems. As such, it is important that they are developed by personnel with a good understanding of business requirements, technologies being used and cyber security matters.

System-specific cyber security documentation may be presented in multiple formats, including in wikis or other forms of document repositories. Furthermore, depending on the documentation framework used, details common to multiple systems could be consolidated into higher-level cyber security documentation.

System security plan

The system security plan provides an overview of the system, covering the system’s purpose, the system boundary and how the system is managed, as well as an annex that describes the security controls that have been identified and implemented for the system.

There can be many stakeholders involved in developing and maintaining a system security plan. This can include representatives from the following groups:

- cyber security teams
- project teams who deliver the capability (including contractors)
- support teams who operate and support the capability
- data owners for data processed, stored or communicated by the system
- users for whom the capability is being developed.

Control: ISM-0041; Revision: 7; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A

Systems have a system security plan that includes an overview of the system (covering the system’s purpose, the system boundary and how the system is managed) as well as an annex that covers applicable

security controls from this document and any additional security controls that have been identified and implemented.

Cyber security incident response plan

Having a cyber security incident response plan ensures that when a cyber security incident occurs, a plan is in place to respond appropriately to the situation. In most situations, the aim of the response will be to prevent the cyber security incident from escalating, restore any impacted system or data, and preserve any evidence.

Control: ISM-0043; Revision: 6; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A

Systems have a cyber security incident response plan that covers the following:

- *guidelines on what constitutes a cyber security incident*
- *the types of cyber security incidents likely to be encountered and the expected response to each type*
- *how to report cyber security incidents, internally to an organisation and externally to relevant authorities*
- *other parties that need to be informed in the event of a cyber security incident*
- *the authority, or authorities, responsible for investigating and responding to cyber security incidents*
- *the criteria by which an investigation of a cyber security incident would be requested from a law enforcement agency, the Australian Signals Directorate or other relevant authority*
- *the steps necessary to ensure the integrity of evidence relating to a cyber security incident*
- *system contingency measures or a reference to such details if they are in a separate document.*

Change and configuration management plan

Having a change and configuration management plan ensures that changes to the configuration of systems can be made in an accountable manner, with appropriate consultation, consideration and approvals, to maintain the security of such systems. Furthermore, change management and configuration management processes and procedures provide an opportunity for the security impact of changes to configuration of systems to be considered and, if necessary, additional risk management activities to be undertaken.

Control: ISM-0912; Revision: 6; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A

Systems have a change and configuration management plan that includes:

- *the establishment and maintenance of authorised baseline configurations for systems*
- *what constitutes routine and urgent changes to the configuration of systems*
- *how changes to the configuration of systems will be requested, tracked and documented*
- *who needs to be consulted prior to routine and urgent changes to the configuration of systems*
- *who needs to approve routine and urgent changes to the configuration of systems*
- *who needs to be notified of routine and urgent changes to the configuration of systems*
- *what additional change management and configuration management processes and procedures need to be followed before, during and after routine and urgent changes to the configuration of systems.*

Continuous monitoring plan

A continuous monitoring plan can assist an organisation in proactively identifying, prioritising and responding to vulnerabilities in systems. Furthermore, undertaking security assessment activities as part of continuous monitoring is important as cyber threats and the effectiveness of security controls change over time.

Three types of security assessment activities that support continuously monitoring the security of systems are vulnerability scans, vulnerability assessments and penetration tests. A vulnerability scan involves using tools to conduct automated checks for known vulnerabilities whereas a vulnerability assessment typically consists of a review of a system's architecture or an in-depth hands-on assessment. In each case, the goal is to identify as many vulnerabilities as possible. A penetration test however is designed to exercise real-world scenarios to achieve a specific goal, such as compromising critical systems or data.

Control: ISM-1163; Revision: 11; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A

Systems have a continuous monitoring plan that includes:

- *conducting security assessment activities to identify vulnerabilities*
- *analysing identified vulnerabilities to determine their potential impact*
- *implementing mitigations based on risk, effectiveness and cost.*

Security assessment report

At the conclusion of a security control assessment for a system, a security assessment report should be produced by the assessor. This will assist the system owner in performing any initial remediation actions as well as guiding the development of the system's plan of action and milestones.

Control: ISM-1563; Revision: 2; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A

At the conclusion of a security control assessment for a system, a security assessment report is produced by the assessor and covers:

- *the scope of the security control assessment*
- *the system's strengths and weaknesses*
- *security risks associated with the operation of the system*
- *the effectiveness of the implementation of security controls*
- *any recommended remediation actions.*

Plan of action and milestones

At the conclusion of a security control assessment for a system, and after the production of a security assessment report by the assessor, a plan of action and milestones should be produced by the system owner. This will assist in tracking any of the system's identified weaknesses and recommended remediation actions identified during the security control assessment.

Control: ISM-1564; Revision: 1; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A

At the conclusion of a security control assessment for a system, a plan of action and milestones is produced by the system owner.

Further information

To assist with the development of system-specific cyber security documentation, a system security plan annex template can be found on the Australian Signals Directorate's [Information security manual](#) webpage.

Further information on cyber security incident response activities can be found in the 'Managing cyber security incidents' and 'Responding to cyber security incidents' sections of the [Guidelines for cyber security incidents](#).

Further information on conducting security assessment activities as part of continuously monitoring the security of systems can be found in the 'Security assessments' section of the [Guidelines for security assurance](#).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2026

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license (<https://creativecommons.org/licenses/by/4.0/>).

For the avoidance of doubt, this means this license only applies to material as set out in this document.



The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license (<https://creativecommons.org/licenses/by/4.0/legalcode.en>).

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (<https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines>).



Australian Government
Australian Signals Directorate

ASD AUSTRALIAN
SIGNALS
DIRECTORATE
ACSC Australian
Cyber Security
Centre