Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Information security manual

Last updated: March 2025

Guidelines for cybersecurity documentation

Development and maintenance of cybersecurity documentation

Cybersecurity strategy

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

Control: ISM-0039; Revision: 7; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
A cybersecurity strategy is developed, implemented and maintained.

Approval of cybersecurity documentation

If cybersecurity documentation is not reviewed and approved by an appropriate authority, system owners risk failing in their duty to ensure that appropriate 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 cybersecurity 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: 5; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Organisational-level cybersecurity documentation is approved by the chief information security officer while system-specific cybersecurity documentation is approved by the system's authorising officer.

Control: ISM-1739; Revision: 0; Updated: Mar-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
A system's security architecture is approved prior to the development of the system.

Maintenance of cybersecurity documentation

Threat environments are dynamic. If cybersecurity documentation is not kept up to date to reflect the current threat environment, policies, processes and procedures may cease to be effective. In such a situation, resources could be devoted to cybersecurity initiatives or investments that have reduced effectiveness or are no longer relevant.

Control: ISM-0888; Revision: 6; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Cybersecurity documentation is reviewed at least annually and includes a 'current as at [date]' or equivalent statement.

Communication of cybersecurity documentation

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

Control: ISM-1602; Revision: 1; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Cybersecurity documentation, including notification of subsequent changes, is communicated to all stakeholders.

Further information

Further information on system-specific cybersecurity documentation, such as a system security plan, cybersecurity 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 following section of these guidelines.

Further information on system registers can be found in the chief information security officer section of the *Guidelines for cybersecurity roles*.

Further information on business continuity and disaster recovery plans can be found in the chief information security officer section of the *Guidelines for cybersecurity roles*.

Further information on cybersecurity communication strategies can be found in the chief information security officer section of the *Guidelines for cybersecurity roles*.

Further information on cybersecurity incident management policy can be found in the managing cybersecurity incidents section of the *Guidelines for cybersecurity incidents*.

Further information on cybersecurity incident registers can be found in the managing cybersecurity incidents section of the *Guidelines for cybersecurity 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 system usage policy can be found in the access to systems and their resources 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 fax machine and multifunction device usage policy can be found in the fax machines and 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 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 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 patching section of the *Guidelines for system management*.

Further information on software registers can be found in the system patching 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 event logging policy can be found in the event logging and monitoring section of the *Guidelines for system monitoring*.

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 web usage policy can be found in the web proxies section of the *Guidelines for gateways*.

Further information on data transfer processes and procedures can be found in the data transfers section of the *Guidelines for data transfers*.

System-specific cybersecurity documentation

System-specific cybersecurity documentation

System-specific cybersecurity documentation, such as a system security plan, cybersecurity 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 cybersecurity matters.

System-specific cybersecurity documentation may be presented in a number of 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 cybersecurity 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 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:

- cybersecurity 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: 6; Updated: Jun-24; Applicability: NC, OS, P, S, TS; Essential Eight: 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 controls from this document and any additional controls that have been identified and implemented.

Cybersecurity incident response plan

Having a cybersecurity incident response plan ensures that when a cybersecurity 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 cybersecurity incident from escalating, restore any impacted system or data, and preserve any evidence.

Control: ISM-0043; Revision: 6; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Systems have a cybersecurity incident response plan that covers the following:

- *guidelines on what constitutes a cybersecurity incident*
- *the types of cybersecurity incidents likely to be encountered and the expected response to each type*
- *how to report cybersecurity incidents, internally to an organisation and externally to relevant authorities*
- *other parties which need to be informed in the event of a cybersecurity incident*
- *the authority, or authorities, responsible for investigating and responding to cybersecurity incidents*
- *the criteria by which an investigation of a cybersecurity 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 cybersecurity incident*
- *system contingency measures or a reference to such details if they are located 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, in order 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: 5; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Systems have a change and configuration management plan that includes:

- *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. Measures to monitor and manage vulnerabilities in systems can also provide an organisation with a wealth of valuable information about their exposure to cyberthreats, as well as assisting them to determine security risks associated with the operation of their systems. Undertaking continuous monitoring activities is important as cyberthreats and the effectiveness of controls will change over time.

Three types of continuous monitoring activities are vulnerability scans, vulnerability assessments and penetration tests. A vulnerability scan involves using software 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 in an attempt to achieve a specific goal, such as compromising critical system components or data. Regardless of the continuous monitoring activities chosen, they should be conducted by suitably skilled personnel independent of the system being assessed. Such personnel can be internal to an organisation or from a third party. This ensures that there is no conflict of interest, perceived or otherwise, and that the activities are undertaken in an objective manner.

Control: ISM-1163; Revision: 10; Updated: Sep-23; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
Systems have a continuous monitoring plan that includes:

- *conducting vulnerability scans for systems at least fortnightly*
- *conducting vulnerability assessments and penetration tests for systems prior to deployment, including prior to deployment of significant changes, and at least annually thereafter*

- *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 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: 1; Updated: Jun-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
At the conclusion of a security assessment for a system, a security assessment report is produced by the assessor and covers:

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

Plan of action and milestones

At the conclusion of a security 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 with tracking any of the system's identified weaknesses and recommended remediation actions identified during the security assessment.

Control: ISM-1564; Revision: 0; Updated: May-20; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
At the conclusion of a security 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 cybersecurity documentation, a system security plan annex template, and an equivalent cloud controls matrix template, are available from the Australian Signals Directorate's *Information security manual* webpage.

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.

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate