



Information Security Manual

Published: 22 June 2023

Guidelines for Security Documentation

Development and maintenance of security documentation

Cyber security strategy

A cyber security strategy sets out an organisation's guiding principles, objectives and priorities for cyber security, typically over a three to 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; Applicability: All; Essential Eight: N/A
A cyber security strategy is developed, implemented and maintained.

Approval of security documentation

If security 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 incident response plan and continuous monitoring plan, is approved by the system's authorising officer prior to the development of the system.

Control: ISM-0047; Revision: 4; Updated: May-19; Applicability: All; Essential Eight: N/A
Organisational-level security documentation is approved by the Chief Information Security Officer while system-specific security documentation is approved by the system's authorising officer.

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

Maintenance of security documentation

Threat environments are dynamic. If 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 a situation, resources could be devoted to cyber security initiatives or investments that have reduced effectiveness or are no longer relevant.

Control: ISM-0888; Revision: 5; Updated: May-19; Applicability: All; Essential Eight: N/A
Security documentation is reviewed at least annually and includes a 'current as at [date]' or equivalent statement.

Communication of security documentation

It is important that once security documentation has been approved, it is published and communicated to all stakeholders. If 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: 0; Updated: Aug-20; Applicability: All; Essential Eight: N/A

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

Further information

Further information on system-specific security documentation, such as a system security plan, incident response 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 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 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 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 ICT equipment management policy can be found in the ICT equipment usage section of the [Guidelines for ICT Equipment](#).

Further information on ICT equipment registers can be found in the ICT equipment usage section of the [Guidelines for ICT Equipment](#).

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

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

Further information on ICT equipment disposal processes and procedures can be found in the ICT equipment disposal section of the [Guidelines for ICT 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 application development section of the [Guidelines for Software Development](#).

Further information on vulnerability disclosure processes and procedures can be found in the application development 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 security documentation

System-specific security documentation

System-specific security documentation, such as a system security plan, incident response 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 security 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 security documentation.

System security plan

The system security plan provides a description of a system and includes an annex that describes the controls that have been identified for the system.

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

- 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: 5; Updated: Jun-22; Applicability: All; Essential Eight: N/A

Systems have a system security plan that includes a description of the system and an annex that covers both applicable controls from this document and any additional controls that have been identified.

Incident response plan

Having an 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: 4; Updated: Dec-21; Applicability: All; Essential Eight: N/A

Systems have an 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 which 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 Cyber Security Centre 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 located in a separate document.*

Continuous monitoring plan

A continuous monitoring plan can assist an organisation in proactively identifying, prioritising and responding to security vulnerabilities. Measures to monitor and manage security vulnerabilities in systems can also provide an organisation with a wealth of valuable information about their exposure to cyber threats, as well as assisting them to determine security risks associated with the operation of their systems. Undertaking continuous monitoring activities is important as cyber threats 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 security 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 security 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: 9; Updated: Jun-23; Applicability: All; 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 security 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: All; 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: All; 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 security documentation, a system security plan annex template, and an equivalent cloud controls matrix template, are available from the Australian Cyber Security Centre's [Information Security Manual](#) webpage.