Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JUNE 2021

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 (an action plan) or investments the organisation plans to make as part of its cyber security program. Without a cyber security strategy, organisations risk failing to adequately plan for and manage security and business risks within their organisation.

Security Control: 0039; Revision: 4; Updated: May-19; Applicability: O, P, S, TS
A cyber security strategy is developed and implemented for the organisation.

Approval of security documentation

If security documentation is not approved, personnel will have difficulty ensuring appropriate policies, processes and procedures are in place. Having approval not only assists in the implementation of policies, processes and procedures, it also ensures personnel are aware of cyber security issues and security risks.

Security Control: 0047; Revision: 4; Updated: May-19; Applicability: O, P, S, TS
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.

Maintenance of security documentation

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

Security Control: 0888; Revision: 5; Updated: May-19; Applicability: O, P, S, TS
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, either initially or following any changes, 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 and their use.

Security Control: 1602; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Security documentation, including notification of subsequent changes, is communicated to all stakeholders.

Further information

Further information on intrusion detection and prevent policy can be found in the ***Guidelines for Cyber Security Incidents***.

Further information on cyber security incident registers can be found in the ***Guidelines for Cyber Security Incidents***.

Further information on ICT equipment and media registers can be found in the ***Guidelines for Physical Security***.

Further information on authorised Radio Frequency devices for SECRET and TOP SECRET area registers can be found in the ***Guidelines for Physical Security***.

Further information on cable registers can be found in the ***Guidelines for Communications Infrastructure***.

Further information on cable labelling process and procedures can be found in the ***Guidelines for Communications Infrastructure***.

Further information on telephone systems usage policy can be found in the ***Guidelines for Communications Systems***.

Further information on fax machine and multifunction device usage policy can be found in the ***Guidelines for Communications Systems***.

Further information on mobile device management policy and mobile device usage policy, as well as mobile device emergency sanitisation process and procedures, can be found in the ***Guidelines for Enterprise Mobility***.

Further information on ICT equipment management policy, as well as ICT equipment sanitisation and disposal processes and procedures, can be found in the ***Guidelines for ICT Equipment***.

Further information on media management policy and removable media usage policy, as well as media sanitisation, destruction and disposal processes and procedures, can be found in the ***Guidelines for Media***.

Further information on system administration process and procedures can be found in the ***Guidelines for System Management***.

Further information on patch management process and procedures can be found in the ***Guidelines for System Management***.

Further information on software registers can be found in the ***Guidelines for System Management***.

Further information on change management process and procedures can be found in the ***Guidelines for System Management***.

Further information on digital preservation policy, as well as data backup and restoration processes and procedures, can be found in the ***Guidelines for System Management***.

Further information on event logging policy, as well as event log auditing process and procedures, can be found in the ***Guidelines for System Monitoring***.

Further information on database registers can be found in the ***Guidelines for Database Systems***.

Further information on email usage policy can be found in the ***Guidelines for Email***.

Further information on network device registers can be found in the ***Guidelines for Networking***.

Further information on web usage policy can be found in the ***Guidelines for Gateways***.

Further information on data transfer process and procedures can be found in the ***Guidelines for Data Transfers***.

System-specific security documentation

System-specific security documentation

System-specific security documentation, such as the system security plan, incident response plan, continuous monitoring plan, security assessment report, and plan of action and milestones, support 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 security matters, the technologies being used and the business requirements of the organisation.

System-specific security documentation may be presented in a number of formats including dynamic content such as wikis, intranets 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 security controls that have been identified and implemented for the system.

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

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

Security Control: 0041; Revision: 3; Updated: Aug-19; Applicability: O, P, S, TS
Systems have a system security plan that includes a description of the system and an annex that covers both security controls from this document (based on the system's classification, functionality and technologies) and any additional security controls that have been identified for the system.

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.

Security Control: 0043; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
Systems have an incident response plan that covers the following:

- *guidelines on what constitutes a cyber security incident*
- *the types of incidents likely to be encountered and the expected response to each type*
- *how to report cyber security incidents, internally to the organisation and externally to the Australian Cyber Security Centre (ACSC)*
- *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 ACSC 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 organisations in proactively identifying, prioritising and responding to security vulnerabilities. Measures to monitor and manage security vulnerabilities in systems can also provide organisations 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 security controls will change over time.

Three types of continuous monitoring activities are vulnerability assessments, vulnerability scans and penetration tests. A vulnerability assessment typically consists of a review of a system's architecture or an in-depth hands-on assessment while a vulnerability scan involves using software tools to conduct automated scans. In each case, the goal is to identify as many security vulnerabilities as possible. A penetration test however is designed to exercise real-world targeted cyber intrusion 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 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.

Security Control: 1163; Revision: 6; Updated: Jun-20; Applicability: O, P, S, TS
Systems have a continuous monitoring plan that includes:

- *conducting vulnerability scans for systems at least monthly*
- *conducting vulnerability assessments or penetration tests for systems at least annually*
- *analysing identified security vulnerabilities to determine their potential impact and appropriate mitigations based on effectiveness, cost and existing security controls*
- *using a risk-based approach to prioritise the implementation of identified mitigations.*

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.

Security Control: 1563; Revision: 0; Updated: May-20; Applicability: O, P, S, TS
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 security controls*
- *any recommended remediation actions.*

Plan of action and milestones

At the conclusion of a security assessment for a system, and 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 following the security assessment.

Security Control: 1564; Revision: 0; Updated: May-20; Applicability: O, P, S, TS
At the conclusion of a security assessment for a system, a plan of action and milestones is produced by the system owner.