Information security manual

Using the *Information security manual*

Last updated: September 2025

Executive summary

Purpose

The purpose of the *Information security manual* (ISM) is to outline a cybersecurity framework that an organisation can apply, using their risk management framework, to protect their information technology and operational technology systems from cyberthreats.

Intended audience

The ISM is intended for chief information security officers (CISOs), chief information officers, cybersecurity professionals and information technology managers.

Authority

The ISM represents the considered advice of the Australian Signals Directorate (ASD). This advice is provided in accordance with ASD's designated functions under the *Intelligence Services Act 2001*.

ASD also provides cybersecurity advice in the form of Australian Communications Security Instructions and other cybersecurity-related publications. In these cases, operating system, application and device-specific advice may take precedence over the advice in the ISM.

Legislation and legal considerations

An organisation is not required as a matter of law to comply with the ISM, unless legislation, or a direction given under legislation or by some other lawful authority, compels them to comply. Furthermore, the ISM does not override any obligations imposed by legislation or law. Finally, if the ISM conflicts with legislation or law, the latter takes precedence.

While the ISM contains examples of when legislation or laws may be relevant for an organisation, there is no comprehensive consideration of such issues. When designing, operating and decommissioning systems, an organisation is encouraged to familiarise themselves with relevant legislation, such as the *Archives Act 1983*, *Privacy Act 1988*, *Security of Critical Infrastructure Act 2018* and *Telecommunications (Interception and Access) Act 1979*.

Cybersecurity principles

The purpose of the cybersecurity principles within the ISM is to provide strategic guidance on how an organisation can protect their information technology and operational technology systems from cyberthreats. These cybersecurity principles are grouped into five functions: govern, identify, protect, detect and respond. An organisation should be able to demonstrate that the cybersecurity principles are being adhered to within their organisation.

Cybersecurity guidelines

The purpose of the cybersecurity guidelines within the ISM is to provide practical guidance on how an organisation can protect their information technology and operational technology systems from cyberthreats. An organisation should consider the cybersecurity guidelines that are relevant to each of the systems they operate.

Applying a risk-based approach to cybersecurity

Using a risk management framework

The risk management framework used by the ISM draws from National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. Broadly, the risk management framework used by the ISM has six steps: define the system, select controls, implement controls, assess controls, authorise the system and monitor the system.

Define the system

Determine the system boundary, business criticality and security objectives for the system based on an assessment of the impact if it were to be compromised.

When embarking upon the design of a system, the system boundary, business criticality and security objectives for the system, based on confidentiality, integrity and availability requirements, should be determined. This will ultimately guide activities, such as selecting and tailoring controls, to meet those security objectives and determine the level of residual security risk that will be accepted before the system is authorised to operate.

Following the determination of the system boundary, business criticality and security objectives for a system, a description of the system and its characteristics should be documented in the system's system security plan.

Select controls

Select controls for the system and tailor them to achieve desired security objectives.

Each cybersecurity guideline discusses security risks associated with the topics it covers. Paired with these discussions are controls that ASD considers to provide efficient and effective mitigations based on their suitability to achieve the security objectives for a system. To assist with selecting and tailoring controls for a system, each control is assigned an applicability marking. For example, 'NC' for the protection of non-classified systems (including both government and non-government systems), 'OS' for the protection of

OFFICIAL: Sensitive systems, 'P' for the protection of PROTECTED systems, 'S' for the protection of SECRET systems and 'TS' for the protection of TOP SECRET systems.

While security risks and controls are discussed in the cybersecurity guidelines, and act as a baseline, they should not be considered an exhaustive list for a specific system type or technology. As such, the cybersecurity guidelines provide an important input into an organisation's risk identification and risk treatment activities however do not represent the full extent of such activities.

While the cybersecurity guidelines can assist with risk identification and risk treatment activities, an organisation will still need to undertake their own risk analysis and risk evaluation activities due to the unique nature of each system, its operating environment and the organisation's risk tolerances.

Following the selection and tailoring of controls for a system, including the identification of any inherited common controls, they should be recorded along with the details of their planned implementation in the system's system security plan annex. In addition, and as appropriate, controls should also be recorded in the system's cybersecurity incident response plan, change and configuration management plan, and continuous monitoring plan.

Finally, the selection of controls for a system, as documented in the system's system security plan annex, should be approved by the system's authorising officer.

Implement controls

Implement controls for the system and its operating environment.

Once suitable controls have been identified for a system, and approved by its authorising officer, they should be implemented. In doing so, the details of their actual implementation, if different from their planned implementation, should be documented in the system's system security plan annex.

Assess controls

Assess controls for the system and its operating environment to determine if they have been implemented correctly and are operating as intended.

In conducting a security assessment, it is important that the assessor, system owner and authorising officer first agree to the scope, type and extent of assessment activities, which may be documented in a security assessment plan, such that any risks associated with the security assessment can be appropriately managed. To a large extent, the scope of the security assessment will be determined by the type of system and controls that have been implemented for the system and its operating environment.

For TOP SECRET systems, including sensitive compartmented information systems, security assessments can be undertaken by ASD assessors (or their delegates). For non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET systems, security assessments can be undertaken by an organisation's own assessors or Infosec Registered Assessors Program (IRAP) assessors. In all cases, assessors should hold an appropriate security clearance and have an appropriate level of experience and understanding of the type of system they are assessing.

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

Authorise the system

Authorise the system to operate based on the acceptance of the security risks associated with its operation.

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, cybersecurity incident response plan, change and configuration management plan, continuous monitoring plan, security assessment report, and plan of action and milestones.

In some cases, the security risks associated with a system's operation will be acceptable and it will be granted an ongoing authorisation to operate. However, in other cases the security risks associated with the operation of a system may be unacceptable. In such cases, the authorising officer may request further work be undertaken by the system owner. In the intervening time, the authorising officer may choose to grant authorisation to operate but with constraints placed on the system's use, such as limiting the system's functionality or specifying an expiration date for authorisation to operate. Finally, if the authorising officer deems the security risks to be unacceptable, regardless of any potential constraints placed on the system's use, they may deny authorisation to operate until such time that sufficient remediation actions, if possible, have been completed to an acceptable standard.

For TOP SECRET systems, including sensitive compartmented information systems, the authorising officer is Director-General ASD (or their delegate). For non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET systems, the authorising officer is an organisation's CISO (or their delegate).

For multinational and multi-organisation systems, the authorising officer should be determined by a formal agreement between the parties involved.

For commercial providers providing services to an organisation, the authorising officer is the CISO of the supported organisation (or their delegate).

In all cases, the authorising officer should have an appropriate level of seniority and understanding of security risks they are accepting on behalf of their organisation. In cases where an organisation does not have a CISO, the authorising officer could be a chief security officer, a chief information officer or other senior executive within the organisation.

Monitor the system

Monitor the system, and associated cyberthreats, security risks and controls, on an ongoing basis.

Real-time monitoring of cyberthreats, security risks and controls associated with a system and its operating environment, as outlined in a continuous monitoring plan, is essential to maintaining its security posture. In doing so, specific events may necessitate additional risk management activities. Such events may include:

- changes in security policies relating to the system
- detection of new or emerging cyberthreats to the system or its operating environment
- the discovery that controls for the system are not as effective as planned
- a major cybersecurity incident involving the system
- major architectural changes to the system.

Following the implementation or modification of any controls as a result of risk management activities, another security assessment should be completed. In doing so, the system's authorisation package should be updated. This in turn allows the authorising officer to make an informed risk-based decision as to whether the security risks associated with the system's operation are still acceptable. If the security risks are no longer acceptable, the authorising officer may choose to either place constraints on the system's use, such as introducing or amending an expiration date for authorisation to operate, or revoke authorisation to operate altogether.

Further information

Further information on various risk management frameworks and practices can be found in the following publications:

- International Organization for Standardization (ISO) 31000:2018, *Risk management – Guidelines*
- International Electrotechnical Commission 31010:2019, *Risk management – Risk assessment techniques*
- ISO/International Electrotechnical Commission 27005:2022, *Information security, cybersecurity and privacy protection – Guidance on managing information security risks*
- NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessments*
- NIST SP 800-37 Rev. 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.

Further information on the purpose of IRAP is available from ASD.

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

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