Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Information Security Manual

DECEMBER 2021

Using the Information Security Manual

Executive summary

Purpose

The purpose of the *Information Security Manual* (ISM) is to outline a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and data from cyber threats.

Intended audience

The ISM is intended for Chief Information Security Officers (CISOs), Chief Information Officers, cyber security professionals and information technology managers.

Authority

The ISM represents the considered advice of the Australian Cyber Security Centre (ACSC) within the Australian Signals Directorate (ASD). This advice is provided in accordance with ASD's designated functions under section 7(1)(ca) of the *Intelligence Services Act 2001*.

The ACSC also provides cyber security advice in the form of Australian Communications Security Instructions and other cyber security-related publications. In these cases, device and application-specific advice may take precedence over the advice in the ISM.

Legislation and legal considerations

Organisations are 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 organisations, there is no comprehensive consideration of such issues. When designing, operating and decommissioning systems, organisations are encouraged to familiarise themselves with legislation such as the *Archives Act 1983*, *Privacy Act 1988* and *Telecommunications (Interception and Access) Act 1979*.

Cyber security principles

The purpose of the cyber security principles within the ISM is to provide strategic guidance on how organisations can protect their systems and data from cyber threats. These cyber security principles are grouped into four key activities:

govern, protect, detect and respond. Organisations should be able to demonstrate that the cyber security principles are being adhered to within their organisation.

Cyber security guidelines

The purpose of the cyber security guidelines within the ISM is to provide practical guidance on how organisations can protect their systems and data from cyber threats. These cyber security guidelines cover governance, physical security, personnel security, and information and communications technology security topics. Organisations should consider the cyber security guidelines that are relevant to each of the systems they operate.

Further information

The ISM, including all supporting material, is regularly reviewed and updated. The latest release of the ISM is available from the ACSC.

Applying a risk-based approach to cyber security

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 security controls, implement security controls, assess security controls, authorise the system and monitor the system.

Define the system

Determine the type, value 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 type, value 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 security controls to meet those security objectives and determining the level of residual security risk that will be accepted before the system is authorised to operate.

Following the determination of the type and value of a system, along with its security objectives, a description of the system and its characteristics should be documented in the system's system security plan.

Select security controls

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

Each cyber security guideline discusses security risks associated with the topics it covers. Paired with these discussions are security controls that the ACSC considers to provide efficient and effective mitigations based on their suitability to achieve the security objectives for a system.

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

While the cyber security guidelines can assist with risk identification and risk treatment activities, organisations 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 security controls for a system, 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, security controls should also be recorded in both the system's incident response plan and continuous monitoring plan.

Implement security controls

Implement security controls for the system and its operating environment.

Once suitable security controls have been identified and agreed upon for a system, 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 security controls

Assess security 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 assessors and system owners 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 security 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). While for SECRET and below 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 security 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, incident response 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 authorisation to operate; however, in other cases the security risks associated with operation of a system may be unacceptable. In such cases, the authorising officer may request further work, and potentially another security assessment, 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. Finally, if the authorising officer deems the security risks to be unacceptable regardless of any potential constraints 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, and systems that process, store or communicate sensitive compartmented information, the authorising officer is Director-General ASD or their delegate; while for SECRET and below 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 organisations, 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 cyber threats, security risks and security controls, on an ongoing basis.

Regular monitoring of cyber threats, security risks and security 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 cyber threats to the system or its operating environment
- the discovery that security controls for the system are not as effective as planned
- a major cyber security incident involving the system
- major architectural changes to the system.

Following the implementation or modification of any security 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, and whether to grant ongoing authorisation to operate.

Further information

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

- International Organization for Standardization (ISO) 31000:2018, *Risk management – Guidelines*
- ISO Guide 73:2009, *Risk management – Vocabulary*
- International Electrotechnical Commission 31010:2019, *Risk management – Risk assessment techniques*
- ISO/International Electrotechnical Commission 27005:2018, *Information technology – Security techniques – Information security risk management*
- 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, and a list of current IRAP assessors, is available from the ACSC.