Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

AUGUST 2019

The Australian Government Information Security Manual

Executive summary

Purpose

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

Intended audience

The ISM is intended for Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), 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 paragraph (1)(ca) of section 7 of the ***Intelligence Services Act 2001***.

The ACSC also provides cyber security advice in the form of hardening guides, consumer guides, 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.

Cyber security principles

The ISM is based on a set of foundational cyber security principles centred on four key activities: govern, protect, detect and respond. These principles, which are currently under review, set the strategic framework for protecting information and systems from cyber threats.

Cyber security guidelines

The ISM contains various cyber security guidelines. These guidelines cover governance, physical security, personnel security, and information and communications technology security as they relate to the protection of information and systems. When designing systems, organisations should use the cyber security guidelines that are relevant to the system being designed.

Further information

The complete ISM, including all supporting materials and changes documents, is constantly being reviewed and updated. The latest release can be found at https://www.cyber.gov.au/ism.

Additional cyber security-related publications from the ACSC can be found at https://www.cyber.gov.au/publications.

Applying a risk-based approach to cyber security

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***. Within this risk management framework, the identification of security risks and selection of security controls can be undertaken using a variety of risk management standards, such as International Organization for Standardization (ISO) 31000:2018, ***Risk management – Guidelines***. 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 value of the system, and the information it processes, stores and communicates, based on an assessment of the impact if it were to be compromised.

When embarking upon the design of a system, the value of the system, and the information it processes, stores and communicates, should be determined. This will ultimately guide activities such as the selection of security controls for the system and the level of residual risk that will be accepted before the system is authorised to operate.

To assist in determining the impact of information compromise, the Attorney-General's Department (AGD)'s ***Protective Security Policy Framework*** (PSPF) provides guidance within Table 2 (***Business Impact Levels tool – Assessing damage to the national interest, organisations or individuals***) of their ***Sensitive and classified information*** policy. For organisations that do not handle government information, security controls marked as OFFICIAL and OFFICIAL: Sensitive can be used for a baseline level of protection while those marked as PROTECTED can be used for an increased level of protection.

Select security controls

Using a risk assessment, select security controls for the system and tailor them to achieve an acceptable residual risk.

While the cyber security guidelines don't articulate discrete risk statements, each cyber security guideline discusses security risks associated with the topic it covers. Paired with these discussions are security controls that the ACSC considers to provide efficient and effective mitigations based on the value of a system, and the information it processes, stores and communicates.

While security risks are discussed in the cyber security guidelines, these 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.

Implement security controls

Implement security controls and document how they are implemented within the system and its operating environment.

Once suitable security controls have been identified for a system, they should be implemented and documented within the system's security documentation.

Assess security controls

Assess security controls for the system and its 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 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. However, value also exists in an unfettered search for security vulnerabilities within the system and its operating environment.

For TOP SECRET systems, security assessments can be undertaken by ACSC assessors or Information Security Registered Assessors Program (IRAP) assessors. While for SECRET and below systems, security assessments can be undertaken by an organisation's own assessors or 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 effectiveness of the implementation of security controls, the system's strengths and weaknesses, any recommended remediation activities, and an assessment of security risks associated with the operation of the system.

Authorise the system

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

Before a system is authorised to operate, an authorising officer should formally accept the security risks associated with its operation. In some cases however, security risks may be inadequately identified or security controls may be inadequately implemented. 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 authorise a system to operate for an interim period with caveats placed on its use.

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. While 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 CIO 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 is essential to maintaining its security posture. In doing so, specific events may necessitate additional risk assessments. 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 any additional risk assessments, and the implementation or modification of any security controls, a security assessment should be completed. Once the security assessment has been completed, an authorising officer should authorise the continued operation of the system if appropriate to do so.

Further information

Further information on the use of protective markings can be found in AGD's PSPF, ***Sensitive and classified information*** policy, at https://www.protectivesecurity.gov.au/information/sensitive-classified-information/.

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

- Department of Finance's, ***Commonwealth Risk Management Policy***, at https://www.finance.gov.au/comcover/risk-management/the-commonwealth-risk-management-policy/
- AGD's PSPF, ***Security planning and risk management*** policy, at https://www.protectivesecurity.gov.au/governance/security-planning-risk-management/
- ISO 31000:2018, ***Risk management – Guidelines***, at https://www.iso.org/standard/65694.html
- ISO Guide 73:2009, ***Risk management – Vocabulary***, at https://www.iso.org/standard/44651.html
- International Electrotechnical Commission 31010:2009, ***Risk management – Risk assessment techniques***, at https://www.iso.org/standard/51073.html
- ISO 27005:2018, ***Information technology – Security techniques – Information security risk management***, at https://www.iso.org/standard/75281.html
- NIST SP 800-30 Rev. 1, ***Guide for Conducting Risk Assessments***, at https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final
- NIST SP 800-37 Rev. 2, ***Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy***, at https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final.

The IRAP website lists the range of activities IRAP assessors are authorised to perform. This information is available at https://www.cyber.gov.au/programs/irap.