Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JANUARY 2019

Cyber security framework

Using the cyber security guidelines

Purpose

The purpose of this document is to assist organisations in using their risk management framework to protect their information and systems from cyber threats. While there are other standards and guidelines designed to protect information and systems, the advice in this document is based on the experience of the Australian Cyber Security Centre (ACSC) and the Australian Signals Directorate (ASD).

Authority

Paragraph (1)(ca) of section 7 of the ***Intelligence Services Act 2001*** states that one of ASD's designated functions is:

to provide material, advice and other assistance to any person or body mentioned in subsection (2) on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means; and

Furthermore, subsection (2) of section 7 of the ***Intelligence Services Act 2001*** states:

For the purposes of paragraph (1)(ca), material, advice and other assistance may be provided to the following:

(a) a Commonwealth authority;

(b) a State authority;

(c) a foreign person or entity;

(d) any other person or body if:

> *(i) the material, advice and other assistance are provided for the purpose of protecting or facilitating trade and commerce with other countries, among the States, between Territories or between a Territory and a State, or outside Australia; or*
>
> *(ii) the material, advice and other assistance are provided by way of a postal, telegraphic, telephonic or other like service (within the meaning of paragraph 51(v) of the Constitution); or*
>
> *(iii) the information was obtained or generated in the operation of a postal, telegraphic, telephone or other like service (within the meaning of paragraph 51(v) of the Constitution).*

This document represents the considered advice of the ACSC provided in accordance with ASD's designated functions.

Intended audience

This document is intended for Chief Information Security Officers (CISOs), Chief Information Officers (CIOs), cyber security professionals and information technology managers. As such, this document discusses both governance and technical concepts in order to support the protection of organisations' information and systems.

The ACSC provides further cyber security advice in the form of hardening guides, consumer guides, Australian Communications Security Instructions (ACSIs), and other PROTECT and ALERT publications. In these cases, device and application-specific advice may take precedence over the security controls in this document.

Risk management considerations

This document is not a compliance-based standard. Rather, organisations are encouraged to consider security risks discussed in this document and apply security controls where appropriate within a risk management framework in accordance with their business requirements and threat environment.

Legislation and legal considerations

Organisations are not required as a matter of law to comply with this document, unless legislation, or a direction given under legislation or by some other lawful authority, compels them to comply.

This document does not override any obligations imposed by legislation or law. Furthermore, if this document conflicts with legislation or law, the latter takes precedence.

While this document contains examples of when legislation or laws may be relevant for organisations, there is no comprehensive consideration of such issues.

Applicability of security controls

Each security control in this document has an applicability marking that indicates the information, systems and/or areas that it is applicable to. These applicability markings are based on protective markings from the Attorney-General's Department (AGD)'s ***Protective Security Policy Framework*** (PSPF):

- O: OFFICIAL (including OFFICIAL: Sensitive)
- P: PROTECTED
- S: SECRET
- TS: TOP SECRET.

Organisations that do not handle government information can implement security controls marked as OFFICIAL for a baseline level of protection, or those marked as PROTECTED for an increased level of protection.

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, ***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/

- International Organization for Standardization (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 (IEC) 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
- National Institute of Standards and Technology (NIST) Special Publication (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. 1, ***Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach***, at https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final.