Using the Australian Government Information Security Manual

Executive summary

Legislation and legal considerations

- The content was modified to include references to legislation that organisations should familiarise themselves with when designing, operating and decommissioning systems within their organisations.

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*.

Guidelines for Cyber Security Roles

System owners

System ownership and oversight

- The ‘system ownership’ topic was changed to ‘system ownership and oversight’.
- Security control 1525 was moved from under the ‘gaining authorisation to operate systems’ topic heading to under the ‘system ownership and oversight’ topic heading.
- Security control 1525 was modified to align with language from related security controls.

  *Security Control: 1525; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS*
  System owners register each system with the system’s authorising officer.

  *Security Control: 1525; Revision: 1; Updated: Jan-21; Applicability: O, P, S, TS*
  System owners register each system with its authorising officer.
Protecting systems and their resources

- New ‘protecting systems and their resources’ content, along with four new controls, have been added to reflect the six step risk management framework.

Broadly, the risk management framework used by the *Australian Government Information Security Manual* has six steps: define the system, select security controls, implement security controls, assess security controls, authorise the system and monitor the system. System owners are responsible for the implementation of this six step risk management framework for each of their systems.

- Security Control: 1633; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS
  System owners determine the type, value and security objectives for each system based on an assessment of the impact if it were to be compromised.

- Security Control: 1634; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS
  System owners select security controls for each system and tailor them to achieve desired security objectives.

- Security Control: 1635; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS
  System owners implement identified security controls within each system and its operating environment.

- Security Control: 1636; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS
  System owners ensure security controls for each system and its operating environment are assessed to determine if they have been implemented correctly and are operating as intended.

- Security control 0027 was moved from under the ‘gaining authorisation to operate systems’ topic heading to under the ‘protecting systems and their resources’ topic heading and was modified to align more closely with the wording of the associated step within the six step risk management framework.

- Security Control: 0027; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
  System owners obtain authorisation to operate each system from the system’s authorising officer.

- Security Control: 0027; Revision: 4; Updated: Jan-21; Applicability: O, P, S, TS
  System owners obtain authorisation to operate each system from its authorising officer based on the acceptance of the security risks associated with its operation.

- Security control 1526 was moved from under the ‘monitoring cyber threats, security risks and security controls’ topic heading to under the ‘protecting systems and their resources’ topic heading and modified to align more closely with the wording of the associated step within the six step risk management framework.

- Security Control: 1526; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
  System owners monitor security risks and the effectiveness of security controls for each system.

- Security Control: 1526; Revision: 1; Updated: Jan-21; Applicability: O, P, S, TS
  System owners monitor each system, and associated cyber threats, security risks and security controls, on an ongoing basis.

- The ‘further information’ content was updated to include a reference to further information on the six step risk management framework.

Further information on using the six step risk management framework can be found in *Using the Australian Government Information Security Manual*. 
Guidelines for Outsourcing

Information technology and cloud services

Outsourced cloud services

- Two new security controls have been added to capture the identification and recording of outsourced cloud services.

**Security Control: 1637; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS**
An outsourced cloud services register is maintained and regularly audited.

**Security Control: 1638; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS**
Outsourced cloud services registers contain the following for each outsourced cloud service:

- cloud service provider’s name
- cloud service’s name
- purpose for using the cloud service
- sensitivity or classification of information involved
- due date for the next security assessment of the cloud service
- point of contact for users of the cloud service
- point of contact for the cloud service provider.

Guidelines for Communications Infrastructure

Cable labelling and registration

Cable register

- The ‘cable register’ content was modified slightly.

Maintaining and regularly auditing cable registers allow installers and inspectors to trace cables for malicious or accidental changes or damage. In doing so, cable registers should track all cable management changes throughout the life of a system.

- Security control 0211 was moved from under the ‘cable inspections’ topic heading to the ‘cable register’ topic heading and modified to ensure consistent language with similar security controls such as 0336, 1493, 1243, 1301 and 1637 relating to registers for ICT assets.

**Security Control: 0211; Revision: 4; Updated: May-20; Applicability: O, P, S, TS**
Cables are inspected for inconsistencies with the cable register at least annually.

**Security Control: 0211; Revision: 5; Updated: Jan-21; Applicability: O, P, S, TS**
A cable register is maintained and regularly audited.

- Security control 0208 was modified slightly due to changes to security control 0211.

**Security Control: 0208; Revision: 3; Updated: Dec-19; Applicability: O, P, S, TS**
A cable register is maintained with the following information:
Guidelines for System Hardening

Authentication hardening

Further information

- The content was modified to include a reference to the ACSC’s new Creating Strong Passphrases publication.

Further information creating strong passphrases can be found in the ACSC’s Creating Strong Passphrases publication at https://www.cyber.gov.au/acsc/view-all-content/publications/creating-strong-passphrases.

Virtualisation hardening

Functional separation between computing environments

- Security control 1461 was modified to remove a conflict with security control 1529.

Security Control: 1461; Revision: 2; Updated: Jul-19; Applicability: S, TS
When using a software-based isolation mechanism to share a physical server’s hardware, the physical server and all computing environments running on the physical server are controlled by the same organisation, are of the same classification and are within the same security domain.

Security Control: 1461; Revision: 3; Updated: Jan-21; Applicability: S, TS
When using a software-based isolation mechanism to share a physical server’s hardware, the physical server and all computing environments running on the physical server are of the same classification and within the same security domain.
Guidelines for Email

Email gateways and servers

Further information

- The content was modified to include a reference to the ACSC’s new *Implementing Certificates, TLS, HTTPS and Opportunistic TLS* publication.


Please note: There is no requirement for organisations to be compliant with every monthly update to the *Australian Government Information Security Manual* (ISM). Instead, organisations are encouraged to review the security risks for their systems (using the latest version of the ISM available at the time) based on a frequency suitable for their business requirements and in accordance with their corporate risk management framework. Further information on applying the ISM can be found in the *Using the Australian Government Information Security Manual* chapter.