June 2020 ISM Changes

Summary of key changes

- Introduction of a recommendation to conduct monthly vulnerability scanning activities.
- Introduction of a recommendation to conduct privileged user training.
- Introduction of a recommendation to audit the use of standard accounts and any activities undertaken with them.
- Removal of a recommendation to use multiple different cloud service providers for online content hosting.
- Clarification of recommendations for auditing of data transfers related to sensitive and lesser classified systems.

Using the Australian Government Information Security Manual

Applying a risk-based approach to cyber security

- Inclusion of missing content heading ‘using a risk management framework’.
- Minor changes to existing content headings to add clarity.

Cyber Security Principles

The cyber security principles

- Inclusion of missing content heading ‘purpose of the cyber security principles’.

Guidelines for Security Documentation

Development and maintenance of security documentation

- Minor amendment to ‘further information’ content.

System-specific security documentation

- Security control 1163 was amended to clarify different recommended frequencies for vulnerability scanning activities (at least monthly) versus vulnerability assessments and penetration tests (at least annually).

Security Control: 1163; Revision: 6; Updated: Jun-20; Applicability: O, P, S, TS
Systems have a continuous monitoring plan that includes:

- conducting vulnerability scans for systems at least monthly
- conducting vulnerability assessments or penetration tests for systems at least annually
- analysing identified security vulnerabilities to determine their potential impact and appropriate mitigations based on effectiveness, cost and existing security controls
- using a risk-based approach to prioritise the implementation of identified mitigations.

**Guidelines for Personnel Security**

**Cyber security awareness training**

- Security control 0252 was modified slightly to capture an annual timeframe for cyber security awareness training activities.

  *Security Control: 0252; Revision: 6; Updated: Jun-20; Applicability: O, P, S, TS*

  Cyber security awareness training is undertaken annually by all personnel and covers:

  - the purpose of the cyber security awareness training
  - security appointments and contacts within the organisation
  - authorised use of systems and their resources
  - protection of systems and their resources
  - reporting of cyber security incidents and suspected compromises of systems and their resources.

- Security control 1565 was introduced to cover the provision of tailored privileged user training for all privileged users of systems.

  *Security Control: 1565; Revision: 0; Updated: Jun-20; Applicability: O, P, S, TS*

  Tailored privileged user training is undertaken annually by all privileged users.

- Minor amendment to ‘further information’ content.

**Access to systems and their resources**

- Security control 1566 was introduced to cover the auditing of standard accounts. This mirrors security control 1509 relating to the auditing of privileged accounts.

  *Security Control: 1566; Revision: 0; Updated: Jun-20; Applicability: O, P, S, TS*

  The use of standard accounts, and any activities undertaken with them, are monitored and audited.

**Guidelines for Enterprise Mobility**

**Mobile device usage**

- Minor amendment to ‘further information’ content to replace the reference to ‘govdex’ with ‘GovTEAMS’.

**Guidelines for Media Management**

**Media usage**

- Minor amendment to ‘further information’ content.
Media destruction

- Minor amendment to ‘media destruction equipment’ content to replace the reference to ‘govdex’ with ‘GovTEAMS’.
- Minor amendment to ‘outsourcing media destruction’ content to replace the reference to ‘govdex’ with ‘GovTEAMS’.

Guidelines for System Hardening

Authentication hardening

- Amendment to ‘logon banner’ content to note that a logon banner should be displayed before access is granted to a system, and not strictly after a user has authenticated to a system.

Guidelines for Email Management

Email gateways and servers

- Minor amendment to ‘further information’ content.

Guidelines for Network Management

Service continuity for online services

- Security control 1437 was amended to remove the recommendation to use multiple different cloud service providers for hosting online services. Instead, organisations are recommended to use high availability measures as per security controls 1441 and 1438.

  Security Control: 1437; Revision: 3; Updated: Jun-20; Applicability: O, P
  A cloud service provider is used for hosting online services.

Guidelines for Using Cryptography

ASD Approved Cryptographic Algorithms

- Minor amendment to ‘using ASD Approved Cryptographic Algorithms’ content.
- Security control 0471 was modified to clarify that cryptographic equipment and software that doesn’t implement any AACAs is not suitable for the protection of sensitive or classified information.

  Security Control: 0471; Revision: 6; Updated: Jun-20; Applicability: O, P
  Only AACAs are used by cryptographic equipment and software.

ASD Approved Cryptographic Protocols

- Historically, the ‘using ASD Approved Cryptographic Protocols’ content had referred to using only AACAs when implementing AACPs. However, in 2015 this content changed to using only AACPs when cryptographic equipment or software implemented at least one AACP (to mirror security control 0471’s rationale). This rationale conflicted with security control 0481 though which continued to refer to only using AACAs when implementing AACPs. As the individual sections for each AACP now reflect endorsed algorithms that can be used for each protocol, security control 0481 has been amended to reflect this change and to match its associated rationale.
Security control 0481 was modified to clarify that cryptographic equipment and software that doesn’t implement any AACPs is not suitable for the protection of sensitive or classified information.

Security Control: 0481; Revision: 5; Updated: Jun-20; Applicability: O, P
Only AACPs are used by cryptographic equipment and software.

Transport Layer Security

- Minor amendment to ‘further information’ content.

Guidelines for Gateway Management

Gateways

- Minor amendment to ‘deploying gateways’ content.
- Security control 0631 was modified to clarify logging requirements and remove the reference to authentication which is already covered by security control 0620.

Security Control: 0631; Revision: 6; Updated: Jun-20; Applicability: O, P, S, TS
Gateways:

- are the only communications paths into and out of internal networks
- allow only explicitly authorised connections
- are managed via a secure path isolated from all connected networks (physically at the gateway or on a dedicated administration network)
- log all physical and logical access to their components
- are configured to save logs to a secure logging facility
- have all security controls tested to verify their effectiveness after any changes to their configuration.

- Minor amendment to ‘gateway operations’ content to match the associated security control.
- The ‘further information’ content was amended slightly.

Cross Domain Solutions

- Minor amendment to ‘introduction to cross domain security’ content.
- The ‘further information’ content was amended slightly.

Web proxies

- Split of previous section from ‘web content and connections’ into ‘web proxies’ and ‘web content filters’.
- Content related to ‘web proxies’ was split into ‘using web proxies’ and ‘web proxy authentication and logging’.

Web content filters

- Split of previous section from ‘web content and connections’ into ‘web proxies’ and ‘web content filters’.
- The ‘using web content filters’ content was amended slightly to add clarity.
- The ‘inspection of Transport Layer Security traffic’ content was amended to replace the term ‘personally identifiable information’ with ‘personal information’ as per the Privacy Act 1988.
The ‘further information’ content was amended slightly.

**Guidelines for Data Transfers**

- Rename of chapter from ‘Guidelines for Data Transfers and Content Filtering’ to ‘Guidelines for Data Transfers’ due to the movement of the content filtering section into the ‘Guidelines for Gateway Management’.

**Data transfers**

- Minor amendments to ‘user responsibilities’ content.
- Minor amendments to ‘trusted sources’ content.
- Security control 0665 was amended to reflect that trusted sources can include systems (as reflected by the definition of a trusted source) in the glossary of cyber security terms.
  
  
  **Security Control: 0665; Revision: 5; Updated: Jun-20; Applicability: S, TS**
  Trusted sources are limited to people and systems that have been authorised as such by an organisation’s CISO.

- Security control 0675 was amended to remove ambiguity that was introduced with revision three of the security control.
  
  **Security Control: 0675; Revision: 4; Updated: Jun-20; Applicability: S, TS**
  A trusted source signs all data authorised for export from a system.

- Minor amendments to ‘import of data’ content.
- Minor amendments to ‘export of data’ content.
- Security control 0667 was removed due to it duplicating the content in security controls 1187 and 0669.
- Security controls 1294 and 1295 were amended to focus on recommendations for sensitive and lesser classified systems.
  
  **Security Control: 1294; Revision: 2; Updated: Jun-20; Applicability: O, P**
  When importing data to a system, data transfer logs are partially audited at least monthly.

  **Security Control: 1295; Revision: 2; Updated: Jun-20; Applicability: O, P**
  When exporting data out of a system, data transfer logs are partially audited at least monthly.

- Security controls 0660 and 0673 were amended slightly to remove superfluous language.
  
  **Security Control: 0660; Revision: 6; Updated: Jun-20; Applicability: S, TS**
  When importing data to a system, data transfer logs are fully audited at least monthly.

  **Security Control: 0673; Revision: 6; Updated: Jun-20; Applicability: S, TS**
  When exporting data out of a system, data transfer logs are fully audited at least monthly.

- The ‘further information’ content was amended slightly.

**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.