July 2020 ISM Changes

Summary of key changes

- Introduction of a recommendation to not use high risk suppliers and service providers.
- Introduction of a recommendation to use service providers that have made a commitment to secure practices and have a strong track record of maintaining the security of their systems and services.
- Introduction of a recommendation to implement a shared responsibility model between service providers and organisations.
- Introduction of a recommendation for cloud service providers and their cloud services to undergo a security assessment by an Information Security Registered Assessor Program (IRAP) assessor at least every 24 months.
- Introduction of a recommendation to include a right to audit in contractual arrangements with service providers.
- Introduction of a recommendation that contractual arrangements specify regions or availability zones for cloud services.
- Introduction of a recommendation that contractual arrangements specify that organisations have access to service provider logs relating to their information and services.
- Introduction of a recommendation that contractual arrangements specify that service providers will store information in a portable manner that allows organisations to perform their own backups, service migration or service decommissioning without loss of information.
- Introduction of a recommendation that contractual arrangements specify that organisations are given at least a one month notification period before a service provider ceases the provision of any services.
- Introduction of a recommendation that organisations be immediately notified when a service provider accesses or administers their systems or information in an unauthorised manner.
- Introduction of a recommendation to segregate an organisation’s networks from their service provider’s networks.
- Introduction of a recommendation that organisations be notified when cloud service providers change any configured regions or availability zones for online services.
- Introduction of a recommendation that organisations test service providers’ ability to dynamically scale resources in response to genuine demand spikes or denial-of-service attacks.
- Introduction of a recommendation that online services that have a high availability requirement are able to automatically transition between availability zones.
Introduction of a recommendation for organisations to perform continuous real-time monitoring of the availability of their online services.

Guidelines for Cyber Security Incidents

Reporting cyber security incidents

- Minor change to ‘reporting cyber security incidents’ to note that unplanned outages are a cyber security incident and should be appropriately reported.
- Security control 0141 was amended to ensure consistency of language with similar security controls.

Security Control: 0141; Revision: 4; Updated: Jul-20; Applicability: O, P, S, TS
Service providers report all cyber security incidents to the organisation’s CISO, or one of their delegates, as soon as possible after they occur or are discovered.

- Security controls 1433 and 1434 were expanded to cover all security classifications and moved from the service continuity for online services section of the Guidelines for Network Management in order to more closely align with existing reporting recommendations.

Security Control: 1433; Revision: 2; Updated: Jul-20; Applicability: O, P, S, TS
Organisations and service providers maintain 24x7 contact details for each other in order to report cyber security incidents.

Security Control: 1434; Revision: 2; Updated: Jul-20; Applicability: O, P, S, TS
Organisations and service providers provide each other with additional out-of-band contact details for use when normal communication channels fail.

Guidelines for Outsourcing

Information technology and cloud services

- The ‘cyber supply chain risk management’ content was rewritten.
- Security control 1452 was amended to capture service providers as part of cyber supply chain risk management activities.

Security Control: 1452; Revision: 2; Updated: Jul-20; Applicability: O, P, S, TS
A review of suppliers and service providers, including their country of origin, is performed before obtaining software, hardware or services to assess the potential increase to an organisation’s security risk profile.

- Security control 1567 was introduced to recommend against the use of high risk suppliers and service providers.

Security Control: 1567; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS
High risk suppliers and service providers are not used.

- Security control 1568 was introduced to provide guidance on cyber supply chain risk management activities when choosing service providers for outsourced information technology and cloud services.

Security Control: 1568; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS
Outsourced information technology and cloud services are chosen from service providers that have made a commitment to secure practices and have a strong track record of maintaining the security of their systems and services.

- Security control 1569 was introduced to ensure the use of a shared responsibility model between service providers and organisations.
A shared responsibility model is created between service providers and organisations in order to articulate the security responsibilities of each party.

- Security control 0100 was amended to clarify that the period between security assessments shouldn’t be greater than 24 months, as opposed to two years which could be interpreted as every 36 months if timed correctly.

- Commercial and government gateway services selected by the ACSC undergo a joint security assessment by ACSC and Information Security Registered Assessors Program (IRAP) assessors at least every 24 months.

- Security control 1570 was introduced to provide guidance on the frequency of security assessments by IRAP assessors for cloud service providers and their cloud services.

- Security control 1529 was amended to focus on what types of cloud services can be used for highly classified information.

- Security control 0873 was removed as this security risk is better addressed by other security controls, such as 1452, 1567, 1568 and 1572.

- The ‘contractual security requirements’ content was rewritten.

- Security control 1395 was amended slightly.

- Security control 1571 was introduced to ensure a right to audit is included in contractual arrangements with service providers.

- Security control 1451 was amended to focus on the types of information provided to service providers and that ownership of such information is documented in contractual arrangements.

- Security control 1572 was introduced to ensure that regions or availability zones for cloud services are documented in contractual arrangements.
The regions or availability zones where information will be processed, stored and communicated is documented in contractual arrangements.

- Security control 1573 was introduced to ensure contractual arrangements specify that organisations have access to service provider logs relating to their information and services.
  
  **Security Control: 1573; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS**
  Access to all logs relating to an organisation’s information and services are specified in contractual arrangements.

- Security control 1574 was introduced to ensure contractual arrangements specify that service providers store information in a portable manner that allows organisations to perform their own backups, service migration or service decommissioning without loss of information.
  
  **Security Control: 1574; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS**
  Information entrusted to a service provider is stored in a portable manner that allows organisations to perform backups, service migration or service decommissioning without any loss of information.

- Security control 1575 was introduced to ensure contractual arrangements specify that organisations are given at least a one month notification period before a service provider ceases the provision of any services.
  
  **Security Control: 1575; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS**
  A minimum notification period of one month for the cessation of any services by a service provider is documented in contractual arrangements.

- New ‘access to systems and information by service providers’ content was added.

- Security control 1073 was amended to remove the caveat that it only applied when service provider access occurred from outside of Australian borders.
  
  **Security Control: 1073; Revision: 4; Updated: Jul-20; Applicability: O, P, S, TS**
  An organisation’s systems and information are not accessed or administered by a service provider unless a contractual arrangement exists between the organisation and the service provider to do so.

- Security control 1576 was introduced to ensure the immediate notification of organisations when a service provider accesses or administers their systems or information in an unauthorised manner.
  
  **Security Control: 1576; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS**
  If an organisation’s systems or information are accessed or administered by a service provider in an unauthorised manner, organisations are immediately notified.

- The ‘further information’ content was modified to add a reference to the IRAP webpage.

**Guidelines for System Management**

**System management**

- The ‘secure system administration of cloud services’ content was rewritten to cover a shared responsibility model between organisations and their service providers.

**Change management**

- Security control 1211 was amended to capture the assessment of potential security impacts and notification of any disruptions or outages as part of change management processes.
  
  **Security Control: 1211; Revision: 3; Updated: Jul-20; Applicability: O, P, S, TS**
  A change management process, and supporting change management procedures, is developed and implemented covering:
• identification and documentation of requests for change
• approval required for changes to be made
• assessment of potential security impacts
• notification of any planned disruptions or outages
• implementation and testing of approved changes
• the maintenance of system and security documentation.

Guidelines for Network Management

Network design and configuration

• Security control 1577 was introduced to ensure the segregation of an organisation’s networks from their service provider’s networks.
  
  Security Control: 1577; Revision: 0; Updated: Jul-20; Applicability: O, P, S, TS
  
  Organisation networks are segregated from service provider networks.

Service continuity for online services

• New ‘location policies for online services’ content was added.
• Security control 1578 was introduced to ensure the notification of organisations when cloud service providers change any configured regions or availability zones.
  
  Security Control: 1578; Revision: 0; Updated: Jul-20; Applicability: O, P
  
  Organisations are notified by cloud service providers of any change to configured regions or availability zones.

• New ‘availability planning and monitoring for online services’ content was added.
• Security control 1579 was introduced to ensure the testing of service providers’ ability to dynamically scale resources in response to genuine demand spikes or denial-of-service attacks.
  
  Security Control: 1579; Revision: 0; Updated: Jul-20; Applicability: O, P
  
  Cloud service providers’ ability to dynamically scale resources due to a genuine spike in demand or a denial-of-service attack is tested as part of capacity planning processes.

• Security control 1580 was introduced to ensure the automatic transition between availability zones for online services that have a high availability requirement.
  
  Security Control: 1580; Revision: 0; Updated: Jul-20; Applicability: O, P
  
  Where a high availability requirement exists, online services are architected to automatically transition between availability zones.

• Security control 1441 was amended slightly.
  
  Security Control: 1441; Revision: 2; Updated: Jul-20; Applicability: O, P
  
  Where a requirement for high availability exists, a denial of service mitigation service is used.

• Security control 1581 was introduced to ensure the continuous real-time monitoring of the availability of online services.
  
  Security Control: 1581; Revision: 0; Updated: Jul-20; Applicability: O, P
  
  Organisations perform continuous real-time monitoring of the availability of online services.

• Minor changes to ‘using content delivery networks’ content.
- Changes to ‘denial of service strategies’ content to merge in previous ‘denial-of-service attacks’ content.
- Security control 1431 was amended slightly.  
  Security Control: 1431; Revision: 2; Updated: Jul-20; Applicability: O, P  
  Denial-of-service attack prevention and mitigation strategies are discussed with cloud service providers, specifically:
  - their capacity to withstand denial-of-service attacks
  - any costs likely to be incurred as a result of denial-of-service attacks
  - thresholds for notification of denial-of-service attacks
  - thresholds for turning off online services during denial-of-service attacks
  - pre-approved actions that can be undertaken during denial-of-service attacks
  - denial-of-service attack prevention arrangements with upstream service providers to block malicious traffic as far upstream as possible.
- Security controls 1433 and 1434 were moved to the reporting cyber security incidents section of the Guidelines for Cyber Security Incidents.
- Minor changes to ‘preparing for service continuity’ content.
- The ‘further information’ content was modified to add a reference to the ACSC’s Preparing for and Responding to Denial-of-Service Attacks publication.

Cyber Security Terminology

Glossary of cyber security terms

- Additional of ‘control plane’ and ‘share responsibility model’ definitions.

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.