



Information Security Manual: June 2022 Changes

Published: 16 June 2022

Summary of content changes

Changes for the June 2022 update of the [Information Security Manual](#) (ISM) are covered below.

Video-aware and voice-aware proxies

The ISM previously recommended that when video conferencing or internet protocol telephony traffic passed through a gateway that contained firewalls that the firewalls be video-aware or voice-aware. The scope of this recommendation has now been expanded to cover proxies used in a gateway.

New Security Controls	Modified Security Controls	Rescinded Security Controls
-----------------------	----------------------------	-----------------------------

ISM-0546

Modern security-focused application development practices

In supporting software supply chain security initiatives, a recommendation to use SecDevOps practices was introduced. In doing so, SecDevOps ensures that security is considered before software development activities take place – rather than solely between development and operational activities.

New Security Controls	Modified Security Controls	Rescinded Security Controls
-----------------------	----------------------------	-----------------------------

ISM-1780

Encrypting all data communicated over network infrastructure

In supporting the adoption of zero trust principles, a recommendation to encrypt all data communicated over network infrastructure was introduced. Note, however, when selecting cryptographic equipment or software for this purpose, the assurance required will depend on the sensitivity or classification of the data and the physical security of the environment in which it is being applied. It is also important to note that some protocols cannot be encrypted and are therefore exempt. However, in such situations, where practical and feasible, an organisation should still consider transitioning to the use of alternative protocols that support encryption.

New Security Controls	Modified Security Controls	Rescinded Security Controls
-----------------------	----------------------------	-----------------------------

ISM-1781

ISM-0469

Network-based Intrusion Detection and Prevention Systems

The recommendation to configure NIDS or NIPS in non-internet gateways for anomaly-based detection rather than signature-based detection was removed to allow organisations to configure their NIDS or NIPS as they see fit.

New Security Controls	Modified Security Controls	Rescinded Security Controls
		ISM-1185

Protective Domain Name System Services

In supporting network security activities, a recommendation to use a protective Domain Name System (DNS) service was introduced. A protective DNS service can be an effective way of blocking requests made by an organisation’s users, or an adversary on an organisation’s network, to known malicious domains – either as part of an initial compromise or subsequent command and control activities. DNS event logs captured by a protective DNS service can also be useful for investigating any exploitation attempt or successful compromise of a network by an adversary.

New Security Controls	Modified Security Controls	Rescinded Security Controls
		ISM-1782

Cryptographic key management processes and procedures

The ISM previously recommended the use of key management plans. This recommendation was reintroduced and amended to cover the development and implementation of cryptographic key management processes and procedures for all systems that employ cryptography. Note, specific requirements for cryptographic key management involving High Assurance Cryptographic Equipment (HACE) are covered by the ACSC’s suite of Australian Communications Security Instruction (ACSI) publications.

New Security Controls	Modified Security Controls	Rescinded Security Controls
		ISM-0507

Cryptographic controlled areas

The recommendation to designate areas in which HACE are used as ‘cryptographic controlled areas’ was rescinded. Note, specific requirements for these areas are covered by the ACSC’s suite of ACSI publications.

New Security Controls	Modified Security Controls	Rescinded Security Controls
		ISM-0506

Assessment of gateways and gateway services

The ISM previously recommended that ‘commercial and government gateway services selected by the ACSC undergo a joint security assessment by ACSC and Infosec Registered Assessors Program (IRAP) assessors at least every 24 months’. This recommendation was reintroduced and amended to ‘gateways undergo a security assessment by an IRAP assessor

at least every 24 months’ to support the upcoming release of new gateway security guidance by the ACSC. Note, the scope of this recommendation relates to all gateways, and not just outsourced gateways services.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0100, ISM-1037	

Data analysis and flow analysis for gateways

Previously the ISM recommended logging network traffic permitted through gateways or attempting to leave gateways. This recommendation has been changed to logging data packets and data flows in order to more explicitly define the types of events that should be logged. Logging these events will facilitate data analysis and flow analysis activities for gateways.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0634	ISM-0648

Border Gateway Protocol route security

Resource Public Key Infrastructure (RPKI) uses public key cryptography to authenticate routing data on the internet. This allows an organisation, particularly a telecommunications carrier or cloud service provider, to verify routing data they receive, transmit and process in order to determine routing calculations for internet traffic. By using RPKI, an organisation may reduce Border Gateway Protocol-related cyber threats, such as some types of denial-of-service attacks, accidental or deliberate rerouting of internet traffic, and opportunities for the undermining of IP address-based reputational services. RPKI Route Origin Authorization (ROA) records, which describe routes in terms of network/prefix and Autonomous Systems from which they are expected to originate, should be configured for the public IP addresses controlled by, or used by, an organisation. ROA records should also be configured for the unannounced IP address space controlled by an organisation.

New Security Controls	Modified Security Controls	Rescinded Security Controls
ISM-1783		

Miscellaneous changes

Miscellaneous changes were made to rationale and recommendations throughout the publication to clarify content. This included the adoption of ‘control’ terminology, in preference to ‘security control’ terminology, to allow for the capture of other types of controls in the future, such as privacy controls, in addition to security controls.

In addition, formatting changes were made to the system security plan annex template and the cloud controls matrix template in order to increase their alignment, such as the inclusion of an ‘implementation status’ column within the system security plan annex template. Furthermore, a new ‘responsible entity’ column was added to both templates in order to capture information on the responsible system (in the case of inherited controls) or responsible vendor (in the case of multi-vendor systems) that are responsible for the implementation of controls. Note, this column can also be used to capture information on teams or individuals that are responsible for the implementation of controls if desired.

New Security Controls	Modified Security Controls	Rescinded Security Controls
	ISM-0041, ISM-0195, ISM-0246, ISM-0409, ISM-0411, ISM-0441, ISM-0569, ISM-0571, ISM-0590, ISM-0840, ISM-1080, ISM-1196, ISM-1198, ISM-1199, ISM-1200, ISM-1296, ISM-1361, ISM-1526, ISM-1537, ISM-1563, ISM-1570, ISM-1634, ISM-1635, ISM-1636	

Contact details

If you have any questions regarding this guidance you can [write to us](#) or call us on (02) 5130 0156.