Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Information Security Manual: March 2023 Changes

Published: 02 March 2023

Summary of content changes

Changes to principles and controls for the March 2023 update of the *Information Security Manual* (ISM) are covered below.

Cyber Security Principles

Protect principles

The existing principle relating to systems and applications being 'configured' to reduce their attack surface was amended to 'designed and configured' in order to support the adoption of the secure-by-design principle. [P3]

Guidelines for Cyber Security Incidents

Reporting cyber security incidents

The existing control relating to reporting cyber security incidents to an organisation's Chief Information Security Officer, or one of their delegates, as soon as possible after they occur or are discovered has been mapped to Essential Eight Maturity Level Three of the *Essential Eight Maturity Model* reflecting that this is part of actioning signs of compromise. [ISM-0123]

Reporting cyber security incidents to the ACSC

The existing control relating to reporting cyber security incidents to the Australian Cyber Security Centre has been mapped to Essential Eight Maturity Level Three of the *Essential Eight Maturity Model* reflecting that this is part of actioning signs of compromise. [ISM-0140]

Enacting incident response plans

A new control was added covering an organisation enacting their incident response plan following the identification of a cyber security incident. This control has been mapped to Essential Eight Maturity Level Three of the *Essential Eight Maturity Model* reflecting that this is part of actioning signs of compromise. [ISM-1819]

Maintaining the integrity of evidence

An existing control relating to maintaining the integrity of evidence gathered during investigations was expanded to include advice to follow 'all instructions provided by relevant law enforcement agencies'. [ISM-0138]

Guidelines for Procurement and Outsourcing

Cyber supply chain risk management activities

An existing control relating to choosing applications, ICT equipment and services from ‘suppliers that have made a commitment to the security of their products and services’ was amended to ‘suppliers that have demonstrated a commitment to the security of their products and services’. [ISM-1568]

Guidelines for Security Documentation

Continuous monitoring plan

An existing control relating to continuous monitoring plans was amended such that mitigations for identified security vulnerabilities are implemented based on risk, effectiveness and cost considerations. [ISM-1163]

Guidelines for Personnel Security

Privileged access to systems

An existing control relating to database administrator accounts being used exclusively for database administrative activities was expanded to ensure that unique privileged accounts are used for administration of individual server applications. [ISM-1263]

Guidelines for Communications Infrastructure

Cable colours

A new control was added covering the use of consistent colours for cables belonging to the same system. [ISM-1820]

Existing controls relating to cable colours for SECRET and TOP SECRET cables were amended to fix grammatical errors. [ISM-1718, ISM-1719]

Common cable bundles

An existing control relating to use of individual ‘conduits’ for SECRET and TOP SECRET cabling was amended to ‘cable bundles and conduits’ for SECRET systems. [ISM-0187]

A new control was added to mirror ISM-0187, but instead for cable bundles and conduits for TOP SECRET systems. [ISM-1821]

An existing control relating to fibre optic cables carrying only a single cable group was rescinded due to overlapping coverage with other controls. [ISM-0189]

Common cable reticulation systems

An existing control relating to common cable reticulation systems was amended to note that both cable bundles and conduits, when sharing a common cable reticulation system, need to have a dividing partition or visible gap between each cable bundle and conduit. [ISM-1114]

Wall outlet boxes

An existing control relating to wall outlet boxes having connectors on different sides of the wall outlet box when different systems use the same wall outlet box was rescinded as it provided limited benefit given such connectors should already be individually labelled according to the systems they belong to. [ISM-1104]

An existing control relating to wall outlet boxes not sharing different cable groups was amended to SECRET and TOP SECRET wall outlet boxes containing exclusively SECRET cables or exclusively TOP SECRET cables. [ISM-1105]

Wall outlet box colours

A new control was added covering the use of consistent colours for wall outlet boxes belonging to the same system. [ISM-1822]

Terminating cables in cabinets

An existing control relating to cables being terminated in individual cabinets, or one cabinet with a division plate between cable groups for small systems, was amended to SECRET cables are terminated in an individual cabinet, or one cabinet with a division plate between SECRET cables and non-SECRET cables for small systems. [ISM-1098]

Terminating cables on patch panels

An existing control relating to different cable groups not being terminated on the same patch panel was amended to SECRET and TOP SECRET cables are terminated on their own individual patch panels. [ISM-0213]

Physical separation of cabinets and patch panels

An existing control relating to TOP SECRET patch panels and non-TOP SECRET patch panels being physically separated via installation in separate cabinets was amended to ‘TOP SECRET patch panels are installed in individual TOP SECRET cabinets’ to mirror language from control ISM-1100. [ISM-0216]

An existing control relating to where spatial constraints demand patch panels of ‘lower classifications’ be in the same cabinet as a TOP SECRET patch panel was amended to ‘non-TOP SECRET patch panels’ in the same cabinet as a TOP SECRET patch panel. [ISM-0217]

An existing control relating to visible gaps between TOP SECRET cabinets and cabinets of ‘lower classifications’ was amended to TOP SECRET cabinets and ‘non-TOP SECRET cabinets’. [ISM-1116]

Guidelines for Communications Systems

Cordless telephone systems

An existing control relating to cordless telephone systems not being used for sensitive or classified conversations was amended to cordless telephone handsets and headsets are not used for sensitive or classified conversations unless all communications are appropriately encrypted. [ISM-0233]

Guidelines for Evaluated Products

Evaluated product selection

An existing control relating to the selection of products that have ‘completed a PP-based evaluation’, in preference to those that have ‘completed an EAL-based evaluation’, was amended to ‘completed a PP-based evaluation, including against all applicable PP modules,’. [ISM-0280]

Guidelines for System Hardening

Operating system selection

An existing control relating to choosing operating systems from 'vendors that have made a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products' was amended to 'vendors that have demonstrated a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products'. [ISM-1743]

Application control

An existing control relating to application control where 'only approved users can write to and modify content within approved folders and files' was amended to 'only approved users can modify approved files and write to approved folders'. [ISM-1392]

An existing control relating to 'approved folders and files' for application control was amended to 'approved files and folders' to ensure consistency of language with the preceding control. [ISM-1746]

User application selection

An existing control relating to choosing applications from 'vendors that have made a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products' was amended to 'user applications' and 'vendors that have demonstrated a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products'. [ISM-0938]

Hardening user application configurations

An existing control relating to changing default accounts or credentials for 'applications' was amended to 'user applications'. [ISM-1806]

An existing control relating to preventing users from changing security settings for web browsers, Microsoft Office and PDF software was split into three separate controls to facilitate independent implementation and assessment in accordance with the *Essential Eight Maturity Model*. [ISM-1585, ISM-1823, ISM-1824]

An existing control relating to preventing users from changing security settings for office productivity suites, email clients and security products was split into three separate controls to facilitate independent implementation and assessment. [ISM-1748, ISM-1823, ISM-1825]

Server application selection

A new control was added covering server applications being chosen from vendors that have demonstrated a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products. [ISM-1826]

Server application releases

An existing control relating to the use of the latest release of 'web server applications, and other internet-accessible server applications', was simplified to 'all internet-facing server applications'. [ISM-1483]

Hardening server application configurations

An existing control relating to database management system (DBMS) software being configured according to vendor guidance was expanded to cover all server applications. [ISM-1246]

An existing control relating to default database administrator accounts being disabled, renamed or having their credentials changed was expanded to cover default accounts for all server applications. [ISM-1260]

An existing control relating to unneeded accounts, components, services and functionality of DBMS software being disabled or removed was expanded to cover all server applications. [ISM-1247]

An existing control relating to temporary files and logs created during DBMS software installation was expanded to cover all server applications. [ISM-1245]

Restricting privileges for server applications

An existing control relating to DBMS software being configured to run as a separate account with the minimum privileges needed to perform its functions was expanded to cover all server applications. [ISM-1249]

An existing control relating to DBMS software having limited access to non-essential areas of their underlying database server's file system was expanded to cover all server applications having limited access to their underlying server's file system. [ISM-1250]

An existing control relating to the ability of DBMS software to read local files from its underlying database server was rescinded due to overlap with the expanded scope of ISM-1250. [ISM-1251]

Database administrator accounts

An existing control relating to database administrators having unique and identifiable accounts was rescinded due to duplication of existing controls [ISM-0414, ISM-0415] relating to personnel with access to systems and their resources being either uniquely identifiable, or if not, having shared accounts that are strictly controlled. [ISM-1262]

An existing control relating to database administrator accounts not being shared across databases was rescinded. [ISM-1261]

An existing control relating to database administrator accounts being restricted to defined roles rather that having default permissions or all permissions was rescinded due to duplication of an existing control [ISM-1508] on limiting privileged access to systems and applications to only what is required for users to undertake their duties. [ISM-1264]

Microsoft Active Directory Domain Services domain controllers

Five new controls were added covering Microsoft Active Directory Domain Services (AD DS) domain controllers. [ISM-1827, ISM-1828, ISM-1829, ISM-1830, ISM-1831]

Microsoft Active Directory Domain Services account hardening

Thirteen new controls were added covering Microsoft AD DS account hardening. [ISM-1832, ISM-1833, ISM-1834, ISM-1835, ISM-1836, ISM-1837, ISM-1838, ISM-1839, ISM-1840, ISM-1841, ISM-1842, ISM-1843, ISM-1844]

Microsoft Active Directory Domain Services security group memberships

An existing control covering 'privileged accounts' being members of the Protected Users security group was amended to 'privileged user accounts' and moved from the authentication hardening section to the server application hardening section of the *Guidelines for System Hardening*. [ISM-1620]

Three new controls were added covering the hardening of Microsoft AD DS security group memberships. [ISM-1845, ISM-1846]

Multi-factor authentication

An existing control relating to 'verifier-impersonation resistant' multi-factor authentication was amended to 'phishing-resistant' multi-factor authentication to align with increasingly prevalent industry terminology. [ISM-1682]

Changing credentials

A new control was added covering changing the credentials for the Kerberos Key Distribution Center's service account (KRBTGT) at least twice, allowing for replication to all Microsoft AD DS domain controllers in-between each change, when a domain has been directly compromised, when a domain is suspected of being compromised or when the credentials haven't been changed in the past 12 months. [ISM-1847]

Functional separation between computing environments

An existing control relating to choosing software-based isolation mechanisms from 'vendors that have made a commitment to secure-by-design principles, secure programming practices and maintaining the security of their products' was amended to 'vendors that have demonstrated a commitment to secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, secure programming practices, and maintaining the security of their products'. [ISM-1460]

A new control was added covering replacing software-based isolation mechanisms, or their underlying operating system, when they are no longer supported by vendors. [ISM-1848]

Guidelines for System Monitoring

Event log retention

An existing control relating to the retention period for 'event logs' was reworded to avoid conflicting with another control [ISM-0991] relating to the retention period for 'DNS service and web proxy event logs'. [ISM-0859]

An existing control relating to the retention period for 'DNS service and web proxy' event logs was reworded slightly for consistency of language with the preceding control. [ISM-0991]

Guidelines for Software Development

Secure software design and development

An existing control relating to 'secure-by-design principles and secure programming practices' being used as part of application development was amended to 'secure-by-design and secure-by-default principles, use of memory-safe programming languages where possible, and secure programming practices'. [ISM-0401]

Application security testing

An existing control relating to applications being 'robustly tested for security vulnerabilities' was amended to 'comprehensively tested for security vulnerabilities, using both static application security testing and dynamic application security testing,' to clarify the intent of the control as reflected in its associated rationale. [ISM-0402]

An existing control relating to software developers resolving security vulnerabilities was amended to specify that this should be done in a timely manner. [ISM-1754]

Open Web Application Security Projects

An existing control relating to the use of the *OWASP Application Security Verification Standard* in the development of web applications was reworded without changing its intent. [ISM-0971]

A new control was added covering the use of the *OWASP Top Ten Proactive Controls* in the development of web applications. [ISM-1849]

A new control was added covering the mitigation of the *OWASP Top 10* in the development of web applications. [ISM-1850]

Web application programming interfaces

An existing control relating to authentication of clients calling web application programming interfaces (APIs) that facilitate access to data not authorised for release into the public domain was amended to also include authorisation. [ISM-1817]

An existing control relating to authentication of clients calling web APIs that facilitate modification of data was amended to also include authorisation. [ISM-1818]

A new control was added covering the mitigation of the *OWASP API Security Top 10* in the development of web APIs. [ISM-1851]

Guidelines for Database Systems

Database management system software

The DBMS software section within the *Guidelines for Database Systems* was rescinded with applicable content merged into the new server application hardening section within the *Guidelines for System Hardening*.

Web application interaction with databases

An existing control relating to the use of parameterised queries or stored procedures for database interactions was reworded to reduce confusion. [ISM-1276]

An existing control relating to web applications being ‘designed’ to provide as little error information as possible about the structure of databases was amended to being ‘designed or configured’ instead. [ISM-1278]

Guidelines for Gateways

Validating file integrity

An existing control relating to validating the ‘digital signature or checksum’ of files imported or exported via gateways or Cross Domain Solutions was amended to validating the ‘digital signature or cryptographic checksum’ instead. [ISM-0677]

Contact details

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