Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Information security manual

Last updated: June 2025

June 2025 changes

A summary of the content changes for the latest update of the *Information security manual* (ISM) are covered below.

Cybersecurity principles

Govern principles

The Govern (GOV) principles were rewritten in support of increased adoption of Secure by Design and Secure by Default principles and practices. Specifically:

- **GOV-01:** The board of directors or executive committee is accountable for cybersecurity.
- **GOV-02:** A chief information security officer provides leadership and oversight of cybersecurity activities.
- **GOV-03:** Security risk management activities for systems (cyber supply chains, infrastructure, operating systems, applications and data) are embedded into organisational risk management frameworks.
- **GOV-04**: Suitable and sufficient personnel and resources are identified and acquired in support of cybersecurity activities.
- **GOV-05:** Security risks for systems (cyber supply chains, infrastructure, operating systems, applications and data) are accepted before they are authorised for use and continuously monitored and managed throughout their operational life.
- **GOV-06:** Security risks for systems (cyber supply chains, infrastructure, operating systems, applications and data) are transparently and mutually communicated with stakeholders.
- **GOV-07:** Security risk management, and associated cybersecurity activities, are regularly reviewed to identify potential improvements in processes and procedures.

Identify principles

The Identify (IDE) principles were rewritten in support of increased adoption of Secure by Design and Secure by Default principles and practices. Specifically:

- **IDE-01:** The business criticality of systems (cyber supply chains, infrastructure, operating systems, applications and data) is determined and documented.

- **IDE-02:** The confidentiality, integrity and availability requirements for systems (cyber supply chains, infrastructure, operating systems, applications and data) are determined and documented.
- **IDE-03:** Security risks for systems (cyber supply chains, infrastructure, operating systems, applications and data) are identified and documented along with any associated risk management decisions.

Protect principles

The Protect (PRO) principles were rewritten in support of increased adoption of Secure by Design and Secure by Default principles and practices. Specifically:

- **PRO-01:** Systems (infrastructure, operating systems and applications) are planned, designed, developed, tested, deployed, maintained and decommissioned according to their business criticality and their confidentiality, integrity and availability requirements.
- **PRO-02:** Systems (infrastructure, operating systems and applications) are planned, designed, developed, tested, deployed, maintained and decommissioned using Secure by Design and Secure by Default principles and practices.
- **PRO-03:** Systems (infrastructure, operating systems, applications and data) are delivered and supported by trusted suppliers.
- **PRO-04:** Systems (infrastructure, operating systems and applications) are configured to reduce their attack surface.
- **PRO-05:** Systems (infrastructure, operating systems, applications and data) are administered in a secure and accountable manner.
- **PRO-06:** Vulnerabilities in systems (cyber supply chains, infrastructure, operating systems, applications and data) are identified and mitigated in a timely manner.
- **PRO-07:** Only trusted and supported operating systems, applications and code can execute on systems.
- **PRO-08:** Data is encrypted at rest and in transit.
- **PRO-09:** Data communicated between different security domains is controlled and inspectable.
- **PRO-10:** Operating systems, applications, settings and data are backed up in a secure and proven manner on a regular basis.
- **PRO-11:** Only trusted and vetted personnel are granted access to systems (cyber supply chains, infrastructure, operating systems, applications and data).
- **PRO-12:** Personnel are granted the minimum access to systems (cyber supply chains, infrastructure, operating systems, applications and data) required to undertake their duties.
- **PRO-13:** Robust and secure identity, credential and access management is used to control access to systems (cyber supply chains, infrastructure, operating systems, applications and data).
- **PRO-14:** Personnel are provided with ongoing cybersecurity awareness training tailored to their duties.
- **PRO-15:** Physical access to systems (infrastructure) is restricted to authorised personnel and monitored for unusual activities.

Detect principles

The Detect (DET) principles were rewritten in support of increased adoption of Secure by Design and Secure by Default principles and practices. Specifically:

- **DET-01:** Security-relevant event logs are centrally collected and stored securely, then analysed in a timely manner to detect cybersecurity events.
- **DET-02:** Security-relevant configuration changes are centrally collected and stored securely, then analysed in a timely manner to detect cybersecurity events.
- **DET-03:** Cybersecurity events are analysed in a timely manner to identify cybersecurity incidents.

Respond principles

The Respond (RES) principles were rewritten in support of increased adoption of Secure by Design and Secure by Default principles and practices. Specifically:

- **RES-01:** Cybersecurity incident response, business continuity and disaster recovery plans support continued business operations during cybersecurity incidents, and the resumption of normal business operations following cybersecurity incidents.
- **RES-02:** Cybersecurity incidents, including associated response activities, are reported internally and externally to relevant bodies and stakeholders in a timely manner.
- **RES-03:** Cybersecurity incidents are contained, eradicated and recovered from in a timely manner.
- **RES-04:** Lessons learnt from cybersecurity incidents are captured, and areas for improvement are identified and actioned in a timely manner.
- **RES-05:** Security risks for systems (cyber supply chains, infrastructure, operating systems, applications and data) are accepted prior to the resumption of normal business operations following cybersecurity incidents.

Maturity modelling

The maturity model provided for the assessment of the implementation of the cybersecurity principles was rescinded.

Guidelines for cybersecurity roles

Identifying critical business assets

The existing control *the board of directors or executive committee understands the business criticality of their organisation's systems, applications and data, including at least a basic understanding of what exists, their value, where they reside, who has access, who might seek access, how they are protected, and how that protection is verified* was amended to simply refer to 'systems' to ensure consistency of language while noting that applications and data are integral components of systems. **[ISM-2005]**

Overseeing cybersecurity personnel

A new control was added recommending that *the CISO ensures sufficient cybersecurity personnel, with the right skills and experience, are acquired to support cybersecurity activities within their organisation*. **[ISM-2020]**

Protecting systems and their resources

The existing control recommending that *agencies must identify and analyse security risks to their information and systems* was reintroduced and amended to *system owners, in consultation with each system's authorising officer, conduct a threat and risk assessment for each system*. **[ISM-1203]**

The existing control recommending that *agencies must determine system-specific security risks that could warrant additional controls to those specified in this manual* was reintroduced and amended to *system owners, in consultation with each system's authorising officer, identify any supplementary controls required based upon the unique nature of each system, its operating environment and the organisation's risk tolerances*. **[ISM-0009]**

A new control was added recommending that *system owners implement and maintain data minimisation practices for each of their systems*. **[ISM-2021]**

Guidelines for procurement and outsourcing

Cyber supply chain risk management activities

Existing controls referring to the procurement of applications were expanded to capture the procurement of operating systems. **[ISM-1452, ISM-1568, ISM-1631, ISM-1632, ISM-1882]**

The existing control recommending *applications, IT equipment, OT equipment and services are procured from suppliers that have a strong track record of maintaining the security of their own systems and cyber supply chains* was amended to simply refer to 'systems' to ensure consistency of language while noting that cyber supply chains are integral components of systems. **[ISM-1632]**

Sourcing operating systems, applications, IT equipment, OT equipment and services

Existing controls referring to the sourcing of applications were amended to capture the sourcing of operating systems. **[ISM-1787, ISM-1788]**

Delivery of operating systems, applications, IT equipment, OT equipment and services

Existing controls referring to the delivery of applications were amended to capture the delivery of operating systems. **[ISM-1790, ISM-1791, ISM-1792]**

Access to systems by service providers

The existing control recommending *an organisation's systems, applications and data are not accessed or administered by a service provider unless a contractual arrangement exists between the organisation and the service provider to do so* was amended to simply refer to 'systems' to ensure consistency of language while noting that applications and data are integral components of systems. **[ISM-1073]**

The existing control recommending *if an organisation's systems, applications or data are accessed or administered by a service provider in an unauthorised manner, the organisation is immediately notified* was amended to simply refer to 'systems' to ensure consistency of language while noting that applications and data are integral components of systems. **[ISM-1576]**

Guidelines for cybersecurity documentation

Change and configuration management plan

The previously reintroduced control on change management processes was amended to include a reference to the establishment and maintenance of authorised baseline configurations for systems. Specifically:

Systems have a change and configuration management plan that includes:

- *the establishment and maintenance of authorised baseline configurations for systems*
- *what constitutes routine and urgent changes to the configuration of systems*
- *how changes to the configuration of systems will be requested, tracked and documented*
- *who needs to be consulted prior to routine and urgent changes to the configuration of systems*
- *who needs to approve routine and urgent changes to the configuration of systems*
- *who needs to be notified of routine and urgent changes to the configuration of systems*
- *what additional change management and configuration management processes and procedures need be to followed before, during and after routine and urgent changes to the configuration of systems.* **[ISM-0912]**

Guidelines for personnel security

Providing cybersecurity awareness training

A new control was added recommending that *a cybersecurity awareness training register is developed, implemented and maintained*. **[ISM-2022]**

Suspension of access to systems

The existing control recommending that *access to data repositories is disabled after 45 days of inactivity* was rescinded due to its duplication of recommendations within ISM-1404 (for unprivileged access) and ISM-1648 (for privileged access). **[ISM-1716]**

Guidelines for evaluated products

Evaluated product selection

The existing control recommending that *if procuring an evaluated product, a product that has completed a PP-based evaluation, including against all applicable PP modules, is selected in preference to one that has completed an EAL-based evaluation* was amended to include a reference to conducting a software bill of materials assessment (where applicable). **[ISM-0280]**

Guidelines for system hardening

Hardening operating system configurations

The existing control recommending that *default user accounts or credentials for operating systems, including for any pre-configured user accounts, are changed, disabled or removed* was amended to specify that such activities should be conducted during initial setup. **[ISM-0383]**

Hardening user application configurations

The existing control recommending that *default user accounts or credentials for user applications, including for any pre-configured user accounts, are changed, disabled or removed* was amended to specify that such activities should be conducted during initial setup. **[ISM-1806]**

Hardening server application configurations

The existing control recommending that *default user accounts or credentials for server applications, including for any pre-configured user accounts, are changed, disabled or removed* was amended to specify that such activities should be conducted during initial setup. **[ISM-1260]**

Guidelines for software development

Authoritative source for software

A new control was added recommending that *an authoritative source for software is established and maintained*. **[ISM-2023]**

A new control was added recommending that *the authoritative source for software is used for all software development activities*. **[ISM-2024]**

Issue tracking

A new control was added recommending that *an issue tracking solution is used to link software development tasks to security issues and decisions, change or feature requests, programming issues, or bug fixes*. **[ISM-2025]**

Software artefacts

A new control was added recommending that *all software artefacts are scanned for malicious code before being imported into the authoritative source for software, including all compiled code, third-party libraries and software components*. **[ISM-2026]**

A new control was added recommending that *all software artefacts are verified by a digital signature, or a secure hash provided over a secure channel, before being imported into the authoritative source for software*. **[ISM-2027]**

A new control was added recommending that *all imported or referenced third-party software artefacts are tested using static application security testing (SAST), dynamic application security testing (DAST) and software composition analysis (SCA) before being imported into the authoritative source for software and periodically throughout the software development life cycle*. **[ISM-2028]**

A new control was added recommending that *the authoritative source for software restricts the use and import of third-party libraries and software components to trusted sources*. **[ISM-2029]**

A new control was added recommending that *scanning is used during commits to identify plain text or encoded secrets and keys, which are then blocked from being stored in the authoritative source for software*. **[ISM-2030]**

Build solution

A new control was added recommending that *compilers, interpreters and build tools (including pipelines) that provide security features to improve executable file security are implemented and such security features are used*. **[ISM-2031]**

A new control was added recommending that *the build solution ensures that all automated testing is completed without warnings, alerts or errors before building software artefacts*. **[ISM-2032]**

Secure software development

A new control was added recommending that *all software security requirements are documented, stored securely and maintained throughout the software development life cycle*. **[ISM-2033]**

A new control was added recommending that *security design decisions are documented and reviewed throughout the software development cycle*. **[ISM-2034]**

A new control was added recommending that *security roles, responsibilities and knowledge requirements required to support the software development life cycle are identified and documented*. **[ISM-2035]**

A new control was added recommending that *security responsibilities for software developers are identified and documented*. **[ISM-2036]**

A new control was added recommending that *software developers that lack sufficient cybersecurity knowledge and skills required for their projects or tasks undertake suitable training on secure software development and programming practices*. **[ISM-2037]**

A new control was added recommending that *a software developer cybersecurity knowledge and skills register is implemented and maintained*. **[ISM-2038]**

The existing control recommending that *Secure by Design and Secure by Default principles and practices, including secure programming practices and either memory-safe programming languages or less preferably memory-safe programming practices, are used for software development* was split into four separate controls.
[ISM-0401, ISM-2040, ISM-2041, ISM-2042]

A new control was added recommending that *the software threat model is reviewed throughout the software development life cycle to ensure it reflects the as-built software and any changes to the threat environment*.
[ISM-2039]

A new control was added recommending that *software is architected and structured to support readability and maintainability*. **[ISM-2043]**

A new control was added recommending that *software has no default credentials; however, if credentials are required, they are created on first install by the installing organisation*. **[ISM-2044]**

A new control was added recommending that *application backwards compatibility does not compromise any security measures or features*. **[ISM-2045]**

A new control was added recommending that *where software allows user impersonation, sensitive data is not logged and appropriate permissions are set*. **[ISM-2046]**

A new control was added recommending that *where software allows an authentication factor to be reset, the user is notified of the reset through a secondary channel*. **[ISM-2047]**

A new control was added recommending that *where software supports multiple user roles, non-administrative users are prevented from altering their profile permissions or privileges*. **[ISM-2048]**

A new control was added recommending that *when user permissions or credentials are changed, software forces all impacted users to re-authenticate*. **[ISM-2049]**

A new control was added recommending that *when digital signatures are processed by software, they are validated against a certificate trust chain and checked for revocation using a Certificate Revocation List or with the Online Certificate Status Protocol*. **[ISM-2050]**

A new control was added recommending that *software generates sufficient event logs to support the detection of cybersecurity events*. **[ISM-2051]**

A new control was added recommending that *event logs produced by software ensure that any sensitive data is protected*. **[ISM-2052]**

The existing control recommending that *secure configuration guidance is produced as part of software development* was amended to recommended that secure configuration guidance take the form of a hardening guide or loosening guide. **[ISM-1798]**

A new control was added recommending that *end of life procedures for software, covering how to remove the software and how to archive or destroy any user accounts and data, are produced and made available to consumers*. **[ISM-2053]**

Software bill of materials

A new control was added recommending that *if a software bill of materials is available for imported third-party software components, it is used during software development to ensure such software components have no known vulnerabilities*. **[ISM-2054]**

Software build provenance

A new control was added recommending that *if a software build provenance is available for imported third-party software components, it is used during software development to ensure such software components are built to an appropriate standard*. **[ISM-2055]**

A new control was added recommending that *a software build provenance is produced and made available to consumers of software*. **[ISM-2056]**

Software input handling

The existing control recommending that *validation or sanitisation is performed on all input received over the internet by software* was amended to recommend that both validation and sanitisation be performed. **[ISM-1240]**

The existing control recommending that *validation or sanitisation is performed on all input received over a local network by software* was amended to recommend that both validation and sanitisation be performed. **[ISM-2016]**

A new control was added recommending that *all input validation rules are documented, matched in code and tested with both positive and negative unit testing or integration testing*. **[ISM-2057]**

A new control was added recommending that *data sources and serialised data inputs are validated before being deserialised*. **[ISM-2058]**

A new control was added recommending that *file uploads or input are restricted to specific file types, with malicious content scanning occurring prior to file access, file execution or file storage*. **[ISM-2059]**

Software security testing

The existing control recommending that *software is comprehensively tested for vulnerabilities, using static application security testing and dynamic application security testing, prior to their initial release and any subsequent releases* was amended to include a recommendation that software composition analysis be included as part of security testing and that security testing also be conducted periodically in order to attempt to identify any previously unidentified vulnerabilities. **[ISM-0402]**

A new control was added recommending that *code reviews are utilised to ensure software meets Secure by Design principles and practices as well as secure programming practices*. **[ISM-2060]**

A new control was added recommending that *software developer-supported security-focused peer reviews are conducted on all critical and security-focused software components*. **[ISM-2061]**

A new control was added recommending that *unit testing and integration testing, covering both positive and negative use cases, are used to ensure code quality and security*. **[ISM-2062]**

Reporting and resolving vulnerabilities

The existing control recommending that *vulnerabilities identified in software are publicly disclosed (where appropriate to do so) by software developers in a timely manner* was amended to recommend that when vulnerabilities are publicly disclosed that they include Common Weakness Enumeration and Common Platform Enumeration information. **[ISM-1908]**

Software event logging

The existing control recommending that *software crashes and error messages are centrally logged* was amended to clarify that only security-relevant software crashes and error messages need to be logged. **[ISM-1911]**

Secure web application design and development

A new control was added recommending that *if supported, web application session cookies set the HttpOnly flag, Secure flag and the SameSite flag by default*. **[ISM-2063]**

A new control was added recommending that *web application session cookies contain only digitally signed opaque bearer tokens*. **[ISM-2064]**

A new control was added recommending that *web application session cookies using opaque bearer tokens that are not digitally signed use non-sequential random identifiers with a minimum of 128 bits of entropy, preferably 256 bits of entropy*. **[ISM-2065]**

A new control was added recommending that *web application sessions are centrally managed server side*. **[ISM-2066]**

A new control was added recommending that *web applications that support Single Sign On equally support Single Logout*. **[ISM-2067]**

Guidelines for database systems

Protecting database contents

The existing control recommending that *the need-to-know principle is enforced for database contents through the application of minimum privileges, database views and database roles* was amended to include data tokenisation. **[ISM-1268]**

Guidelines for networking

Functional separation between networked devices and the internet

A new control was added recommending that *internet connectivity for networked devices is strictly limited to those that require access*. **[ISM-2068]**

Default user accounts and credentials for network devices

The existing control recommending that *default user accounts or credentials for network devices, including for any pre-configured user accounts, are changed, disabled or removed* was amended to specify that such activities should be conducted during initial setup. **[ISM-1304]**

Guidelines for cryptography

Communications security doctrine

The existing control recommending that *communications security doctrine produced by ASD for the management and operation of HACE is complied with* was amended to include communications security policy produced by ASD. **[ISM-0499]**

Miscellaneous

A number of existing controls were reworded for clarity without changing their intent.
[ISM-0304, ISM-0343, ISM-0382, ISM-0405, ISM-0407, ISM-0414, ISM-0420, ISM-0430, ISM-0432, ISM-0434, ISM-0435, ISM-0441, ISM-0455, ISM-0457, ISM-0465, ISM-0471, ISM-0481, ISM-0489, ISM-0917, ISM-1027, ISM-1235, ISM-1238, ISM-1272, ISM-1404, ISM-1417, ISM-1418, ISM-1467, ISM-1470, ISM-1507, ISM-1508, ISM-1591, ISM-1592, ISM-1598, ISM-1610, ISM-1647, ISM-1648, ISM-1649, ISM-1670, ISM-1691, ISM-1692, ISM-1693, ISM-1699, ISM-1700, ISM-1704, ISM-1754, ISM-1824, ISM-1852, ISM-1860, ISM-1865, ISM-1901, ISM-1909, ISM-1917]

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate