Information security manual

Cyber security principles

Last updated: March 2026

The cyber security principles

Purpose of the cyber security principles

The purpose of the cyber security principles is to provide strategic guidance on how an organisation can protect their information technology and operational technology systems from cyber threats. These cyber security principles are grouped into six functions:

- **Govern:** Develop and maintain a strong and resilient cyber security culture.
- **Identify:** Identify assets and associated security risks.
- **Protect:** Implement and maintain controls to manage security risks.
- **Detect:** Detect and analyse cyber security events to identify cyber security incidents.
- **Respond:** Respond to cyber security incidents.
- **Recover:** Resume normal business operations following cyber security incidents.

Implementing the cyber security principles

Within each function, the cyber security principles are listed in a logical sequence that reflects how they should be considered for implementation. The numbers used for the cyber security principles are identifiers only and do not indicate an implementation order.

When implementing the cyber security principles, each cyber security principle should be supported by administrative and technical controls proportionate to an organisation's size, complexity, operating environment and risk profile. These controls should be subject to ongoing risk-based monitoring and assurance activities. Where the term 'systems' is used, the elements listed in brackets define the scope of that cyber security principle.

Overall, the cyber security principles are interdependent and must be implemented collectively to achieve comprehensive cyber security outcomes.

Govern cyber security principles

The Govern (GOV) cyber security principles are:

- **GOV-01 – Executive cyber security accountability:** The board of directors or executive committee is accountable for cyber security.
- **GOV-08 – Executive artificial intelligence accountability:** The board of directors or executive committee is accountable for ensuring that artificial intelligence is secure, controllable, human-supervised and used in an ethical and accountable manner.
- **GOV-02 – Cyber security leadership:** A chief information security officer provides leadership and oversight of cyber security activities and delivers regular and timely risk-based reporting to the board of directors or executive committee on their organisation's cyber security posture, the effectiveness of controls, current security risks and emerging cyber threats.
- **GOV-04 – Cyber security resourcing:** Suitable and sufficient personnel and resources are identified, acquired and maintained in support of cyber security activities.
- **GOV-09 – Security risk management responsibilities:** Security risk management responsibilities for an organisation and their suppliers, partners and customers, including any shared responsibilities, are documented and communicated to all relevant parties with accountability arrangements in place to ensure their effective implementation.
- **GOV-03 – Security risk management assurance:** Security risk management activities for an organisation and their systems (infrastructure, operating systems, applications and data) are embedded into organisational risk management frameworks and subject to ongoing monitoring and assurance activities by the board of directors or executive committee.
- **GOV-05 – Security risk acceptance:** Residual security risks for systems (infrastructure, operating systems, applications and data), including inherited and shared security risks, are accepted before they are authorised for use and continuously monitored and managed throughout their operational life.
- **GOV-06 – Security risk communication:** Residual security risks for systems (infrastructure, operating systems, applications and data), including inherited and shared security risks, are transparently and mutually communicated with stakeholders.
- **GOV-10 – System exposure minimisation:** Information about the design, configuration and operation of systems (infrastructure, operating systems, applications and data) is not publicly disclosed or shared externally unless necessary for commercial, legal, regulatory or security purposes, with any disclosure minimised, controlled and logged.
- **GOV-11 – Supplier cyber security assurance:** Systems (infrastructure, operating systems, applications and data) are delivered and supported by trustworthy suppliers whose cyber security practices are independently verified, or otherwise risk-assessed, on a regular basis.
- **GOV-12 – Personnel suitability assurance:** Only personnel whose suitability and trustworthiness have been established, and are subject to ongoing assurance, are granted access to systems (infrastructure, operating systems, applications and data).
- **GOV-13 – Cyber security and safety:** Controls for systems (infrastructure, operating systems, applications and data) do not compromise human, physical or environmental safety.
- **GOV-14 – Legacy system management:** Systems (infrastructure, operating systems, applications and data) that are not capable of meeting cyber security requirements are managed using compensating

controls, along with enhanced monitoring and assurance activities, to maintain an acceptable level of residual risk until they can be decommissioned or replaced.

- **GOV-07 – Continuous cyber security improvement:** Security risk management and associated cyber security activities are continually measured and reviewed using cyber threat intelligence and assurance activities, including exercises informed by real-world cyber threats, to identify, prioritise and incorporate improvements in governance arrangements, shared responsibilities and the effectiveness of controls.

Identify cyber security principles

The Identify (IDE) cyber security principles are:

- **IDE-01 – Asset identification:** Systems (infrastructure, operating systems, applications, identities, credentials and data) are continually and centrally identified and documented.
- **IDE-05 – Asset interdependencies:** Interdependencies between systems (infrastructure, operating systems, applications and data) are continually and centrally identified and documented, including how the compromise of one system could affect the security or business operations of other dependent systems.
- **IDE-02 – Business criticality rating identification:** Business criticality ratings for systems (infrastructure, operating systems, applications and data) are identified and documented.
- **IDE-03 – Security requirement identification:** Security requirements for systems (infrastructure, operating systems, applications and data) are identified and documented.
- **IDE-06 – Resilience requirement identification:** Resilience requirements for systems (infrastructure, operating systems, applications and data) are identified and documented.
- **IDE-04 – Security risk identification:** Security risks for an organisation and their systems (infrastructure, operating systems, applications and data) are identified, including by using current strategic and sector-specific cyber threat intelligence and threat modelling, and are documented along with any associated risk management decisions.

Protect cyber security principles

The Protect (PRO) cyber security principles are:

- **PRO-01 – Secure system lifecycle:** Systems (infrastructure, operating systems and applications) are planned, designed, developed, tested, deployed, maintained and decommissioned according to their business criticality ratings and security and resilience requirements using Secure by Design and Secure by Default principles and practices.
- **PRO-16 – Cyber supply chain security:** Cyber supply chains supporting systems (infrastructure, operating systems, applications and data) are secure, resilient and support effective and coordinated cyber security incident response.
- **PRO-13 – Identity, credential and access management:** Robust and secure identity, credential and access management is used to establish, maintain and control access to systems (infrastructure, operating systems, applications and data) and to support effective detection of identity and credential misuse.

- **PRO-12 – Least privilege access:** Personnel and services are granted the minimum access to systems (infrastructure, operating systems, applications and data) required to undertake their duties.
- **PRO-05 – Secure administration:** Systems (infrastructure, operating systems, applications and data) are administered in a secure, accountable and auditable manner.
- **PRO-04 – Secure configuration management:** Systems (infrastructure, operating systems and applications) are securely configured to approved and maintained baselines, including by reducing attack surfaces and attack paths, with configurations continually monitored and consistently enforced.
- **PRO-06 – Vulnerability management:** Vulnerabilities in systems (infrastructure, operating systems, applications and data) are identified, documented, validated and prioritised for remediation or mitigation in a timely manner, with all remediation and mitigation actions verified for effectiveness.
- **PRO-07 – Trustworthy software:** Systems (operating systems and applications) only permit the execution of software that is supported, verified and authorised.
- **PRO-08 – Data protection:** Data is encrypted and authenticated at rest and in transit using ASD-approved algorithms and protocols to protect its confidentiality and integrity.
- **PRO-17 – Cryptographic agility:** Systems (infrastructure, operating systems and applications) are designed, configured and managed to support timely, prioritised and orderly changes to cryptography, including post-quantum cryptography.
- **PRO-10 – Regular and proven backups:** Systems (infrastructure, operating systems, applications and data) are backed up in a secure and proven manner on a regular basis, including through the validation of restoration capabilities.
- **PRO-18 – Network segmentation and segregation:** Systems (infrastructure, operating systems and applications) are segmented into network zones based on business criticality and trust levels, with only authorised, controlled and monitored inbound and outbound communication paths between network zones permitted.
- **PRO-19 – Operational technology isolation:** Operational technology systems (infrastructure) are logically and physically isolated from information technology systems (infrastructure) and all external infrastructure, with only authorised, controlled and monitored communication paths between systems permitted.
- **PRO-20 – Remote access to operational technology:** Access to operational technology systems (infrastructure, operating systems, applications and data) over untrusted infrastructure is authorised, controlled and monitored.
- **PRO-09 – Content filtering:** Data communicated between different security domains for systems (infrastructure and applications) is controlled and subject to inspection and verification.
- **PRO-14 – Cyber security awareness training:** Personnel are provided with ongoing cyber security awareness training, including operational security considerations, tailored to their duties, access levels and current cyber threats.
- **PRO-15 – Physical access control:** Physical access to facilities and systems (infrastructure and data) is restricted to authorised personnel and monitored for unusual activities.

Detect cyber security principles

The Detect (DET) cyber security principles are:

- **DET-01 – Centralised event logging:** Security-relevant event logs and configuration changes for systems (infrastructure, operating systems, applications and data) are centrally collected, protected against unauthorised modification or deletion, and retained to support effective cyber security event detection and investigation.
- **DET-04 – Baselined high-risk access activities:** Baseline patterns of identity and credential access activities, privileged access activities, and remote access activities are established and maintained for systems (infrastructure, operating systems, applications and data) to enable the detection of anomalous or unexpected behaviour.
- **DET-02 – Cyber security event detection:** Anomalous or unexpected events and behaviours for systems (infrastructure, operating systems, applications and data) are analysed in a timely manner to detect cyber security events.
- **DET-03 – Cyber security incident identification:** Cyber security events are analysed in a timely manner to identify cyber security incidents.
- **DET-05 – Detection capability efficacy:** Cyber security event detection capabilities are regularly evaluated for effectiveness and continuously refined, including by using current strategic and sector-specific cyber threat intelligence, to improve the detection of cyber security events.

Respond cyber security principles

The Respond (RES) cyber security principles are:

- **RES-01 – Cyber security incident planning:** Cyber security incident response, business continuity and disaster recovery plans for systems (infrastructure, operating systems, applications and data) support continued business operations during cyber security incidents, and the resumption of normal business operations following cyber security incidents.
- **RES-05 – Cyber security incident coordination:** Cyber security incident roles and responsibilities are defined, documented and exercised to support the internal and external coordination and management of cyber security incidents, including responsibilities for declaring cyber security incidents and undertaking pre-approved response and recovery activities.
- **RES-03 – Cyber security incident response:** Cyber security incidents are contained, eradicated and recovered from in a timely manner.
- **RES-02 – Cyber security incident reporting:** Cyber security incidents, including associated response and recovery activities, are reported internally and externally to relevant bodies and stakeholders in a timely manner.
- **RES-04 – Cyber security incident insights:** Lessons learnt from cyber security incidents are captured, and areas for improvement are identified, prioritised and actioned in a timely manner.

Recover cyber security principles

The Recover (REC) cyber security principles are:

- **REC-02 – System recovery assurance:** Following cyber security incidents, systems (infrastructure, operating systems, applications and data) are verified through assurance activities to ensure they are secure and capable of supporting the resumption of normal business operations.
- **REC-01 – Business operations resumption:** Residual security risks for systems (infrastructure, operating systems, applications and data), including inherited and shared security risks, are accepted prior to the resumption of normal business operations following cyber security incidents.

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.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre