Information security manual

Guidelines for cyber security roles

Last updated: September 2026

Board of directors and executive committee

Embedding cyber security

To ensure that cyber security is embedded throughout an organisation, it is important that the board of directors or executive committee commits to defining clear roles and responsibilities for cyber security and integrating cyber security throughout all business functions within their organisation. They should also align their organisation's cyber security strategy with their organisation's overarching strategic direction and business strategy and seek regular briefings or reporting on the cyber security posture of their organisation and the threat environment in which it operates.

Control: ISM-1997; Revision: 1; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee defines clear roles and responsibilities for cyber security both within the board of directors or executive committee and broadly within their organisation.

Control: ISM-1998; Revision: 1; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee ensures that cyber security is integrated throughout all business functions within their organisation.

Control: ISM-1999; Revision: 1; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee ensures the cyber security strategy for their organisation is aligned with the overarching strategic direction and business strategy for their organisation.

Control: ISM-2000; Revision: 1; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee seeks regular briefings or reporting on the cyber security posture of their organisation, as well as the threat environment in which they operate, from internal and external subject matter experts.

Championing a positive cyber security culture

To provide cyber security leadership within an organisation, it is important that the board of directors or executive committee champions a positive cyber security culture, including through leading by example.

Control: ISM-2001; Revision: 1; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee champions a positive cyber security culture within their organisation, including through leading by example.

Building cyber security expertise

To assist with embedding cyber security throughout an organisation, it is important that the board of directors or executive committee maintains a sufficient level of cyber security literacy to fulfil both their fiduciary duties and any legislative or regulatory obligations. In addition, the board of directors or executive committee should maintain awareness of key cyber security recruitment activities, retention rates for cyber security personnel, and cyber security skills and experience gaps for their organisation. Finally, the board of directors or executive committee should support the development of cyber security skills and experience for all personnel within their organisation.

Control: ISM-2002; Revision: 1; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee maintains a sufficient level of cyber security literacy to fulfil both their fiduciary duties and any legislative or regulatory obligations.

Control: ISM-2003; Revision: 1; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee maintains awareness of key cyber security recruitment activities, retention rates for cyber security personnel, and cyber security skills and experience gaps within their organisation.

Control: ISM-2004; Revision: 1; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee supports the development of cyber security skills and experience for all personnel via internal and external cyber security awareness raising and training opportunities.

Identifying critical business assets

For the board of directors or executive committee to fulfil both their fiduciary duties and any legislative or regulatory obligations, it is important that they understand the business criticality of their organisation's systems. This includes a basic understanding of what systems exist, their value, where they reside, who has access, who might seek access, how they are protected and how that protection is verified.

Control: ISM-2005; Revision: 2; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee understands the business criticality of their organisation's systems, including at least a basic understanding of what systems exist, their value, where they reside, who has access, who might seek access, how they are protected, and how that protection is verified.

Planning for major cyber security incidents

For the board of directors or executive committee to fulfil both their fiduciary duties and any legislative or regulatory obligations, it is important that they plan for major cyber security incidents, including by participating in exercises, and understand their duties in relation to such cyber security incidents.

Control: ISM-2006; Revision: 2; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The board of directors or executive committee plans for major cyber security incidents, including by participating in exercises, and understands their duties in relation to such cyber security incidents.

Further information

Further information on how the board of directors or executive committee can protect themselves from cyber threats can be found in the Australian Signals Directorate's (ASD) *Practical cyber security tips for business leaders* publication.

Further information on questions the board of directors or executive committee should be asking of their organisation can be found in ASD's *Ten things to know about data security* publication.

Further information on how the board of directors or executive committee can plan for major cyber security incidents can be found in ASD's *Planning for critical vulnerabilities: What the board of directors needs to know* publication.

Further information on cyber security considerations for the board of directors or executive committee during mergers, acquisitions and Machinery of Government changes can be found in ASD's *Mergers, acquisitions and Machinery of Government changes* publication.

Further information on cyber security responsibilities and duties of the board of directors or executive committee can be found in the United Kingdom's National Cyber Security Centre's Cyber Security Toolkit for Boards.

Chief information security officer

Context

The role of the chief information security officer (CISO) is to anticipate changes in the threat and technology environment and lead proportionate and evidence-based improvements to their organisation's cyber security capabilities. This requires a combination of technical and soft skills, such as business acumen, leadership, communications and relationship building. In support of this, a CISO should adopt a continuous approach to learning and up-skilling to maintain pace with evolving cyber security frameworks and emerging technologies.

The role of the CISO within an organisation should cover both information technology (IT) and operational technology (OT). However, where appropriate and practical to do so, responsibility for OT cyber security may be delegated by the CISO. Within this section, the breadth of responsibilities for IT and OT is collectively referenced under the banner of cyber security.

Providing cyber security leadership and guidance

To provide cyber security leadership and guidance within an organisation (for IT and OT), it is important that the organisation appoints a CISO.

Control: ISM-0714; Revision: 6; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
A CISO is appointed to provide cyber security leadership and guidance for their organisation (covering IT and OT).

Overseeing the cyber security program

The CISO within an organisation is responsible for overseeing their organisation's cyber security program and ensuring compliance with cyber security policy, standards, regulations and legislation. They are likely to work with a chief security officer, a chief information officer and other senior executives within their organisation.

Control: ISM-1478; Revision: 1; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO oversees their organisation's cyber security program and ensures their organisation's compliance with cyber security policy, standards, regulations and legislation.

Control: ISM-1617; Revision: 0; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO regularly reviews and updates their organisation's cyber security program to ensure its relevance in addressing cyber threats and harnessing business and cyber security opportunities.

Control: ISM-1966; Revision: 1; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO develops, implements, maintains and regularly verifies a register of systems used by their organisation.

Control: ISM-0724; Revision: 2; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO implements cyber security measurement metrics and key performance indicators for their organisation.

Coordinating cyber security

The CISO is responsible for ensuring the alignment of cyber security and business objectives within their organisation. To achieve this, they should facilitate communication between cyber security and business stakeholders. This includes translating cyber security concepts and language into business concepts and language, as well as ensuring that business teams consult with cyber security teams to determine appropriate security controls when planning new business projects. Additionally, as the CISO is responsible for the development of their organisation's cyber security program, they are best placed to advise projects on the strategic direction of cyber security within their organisation.

Control: ISM-0725; Revision: 4; Updated: Jun-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO coordinates cyber security and business alignment through a cyber security steering committee or advisory board, comprising key cyber security and business executives, which meets formally and regularly.

Control: ISM-0726; Revision: 2; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO coordinates security risk management activities between cyber security and business teams.

Reporting on cyber security

The CISO is responsible for reporting cyber security matters to their organisation's board of directors or executive committee, as well as their organisation's audit, risk and compliance committee (or equivalent). In doing so, it is important that reporting is done directly by the CISO rather than via other senior executives within their organisation. This ensures reporting remains accurate and free of any conflicts of interest.

Reporting should cover:

- the organisation's security risk profile
- the status of key systems and any outstanding security risks
- any planned cyber security uplift activities
- any recent cyber security incidents
- expected returns on cyber security investments.

Reporting on cyber security matters should be structured by business functions, regions or legal entities and support a consolidated view of an organisation's security risks.

It is important that the CISO can translate security risks into operational risks for their organisation, including financial and legal risks, to enable more holistic conversations about their organisation's risks.

Control: ISM-0718; Revision: 6; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO regularly reports directly to their organisation's board of directors or executive committee on cyber security matters.

Control: ISM-1918; Revision: 0; Updated: Jun-24; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO regularly reports directly to their organisation's audit, risk and compliance committee (or equivalent) on cyber security matters.

Overseeing cyber security incident response activities

To ensure the CISO can accurately report to their organisation's board of directors or executive committee on cyber security matters, it is important they are fully aware of all cyber security incidents within their organisation.

The CISO is also responsible for overseeing their organisation's response to cyber security incidents, including how internal teams respond and communicate with each other during cyber security incidents. In the event of a major cyber security incident, the CISO should be prepared to step into a crisis management role. They should understand how to bring clarity to the situation and communicate effectively with internal and external stakeholders.

Control: ISM-0733; Revision: 2; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO is fully aware of all cyber security incidents within their organisation.

Control: ISM-1618; Revision: 0; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO oversees their organisation's response to cyber security incidents.

Contributing to business continuity and disaster recovery planning

The CISO is responsible for contributing to the development, implementation and maintenance of their organisation's business continuity and disaster recovery plans, with the aim to improve business resilience and ensure the continued operation of critical business processes.

Control: ISM-0734; Revision: 4; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO contributes to the development, implementation and maintenance of business continuity and disaster recovery plans for their organisation to ensure that business-critical services are supported appropriately in the event of a disaster.

Communicating a cyber security vision and strategy

To assist in facilitating cyber security cultural change and awareness within their organisation, across their organisation's cyber supply chain and among their organisation's customers, the CISO should act as a cyber security leader and regularly communicate the cyber security vision and strategy for their organisation. In doing so, a cyber security communications strategy can be helpful in achieving this outcome. As part of this, communication styles and content should be tailored to different target audiences.

Control: ISM-0720; Revision: 3; Updated: Sep-23; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO oversees the development, implementation and maintenance of a cyber security communications strategy to assist in communicating the cyber security vision and strategy for their organisation.

Working with suppliers

The CISO is responsible for ensuring that consistent vendor management processes are applied across their organisation, from discovery through to management. As supplier relationships come with additional security risks, the CISO should assist personnel with assessing cyber supply chain risks and understanding the security impacts of entering into contracts with suppliers.

Control: ISM-0731; Revision: 2; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO oversees cyber supply chain risk management activities for their organisation.

Receiving and managing a dedicated cyber security budget

Receiving and managing a dedicated cyber security budget will ensure the CISO has sufficient access to funding to support their cyber security program, including cyber security uplift activities and responding to cyber security incidents.

Control: ISM-0732; Revision: 2; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO receives and manages a dedicated cyber security budget for their organisation.

Overseeing cyber security personnel

The CISO is responsible for the cyber security workforce within their organisation, including plans to attract, train and retain cyber security personnel. The CISO should also delegate relevant tasks to cyber security managers and other personnel as required to support cyber security activities within their organisation and provide them with adequate authority and resources to perform their duties.

Control: ISM-0717; Revision: 2; Updated: Oct-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO oversees the management of cyber security personnel within their organisation.

Control: ISM-2020; Revision: 1; Updated: Dec-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO ensures sufficient cyber security personnel, with the right skills and experience, are acquired to support cyber security activities within their organisation.

Overseeing cyber security awareness training

To ensure personnel are actively contributing to the security culture of their organisation, a cyber security awareness training program should be developed, implemented and maintained. As the CISO is responsible for cyber security within their organisation, they should oversee the development, implementation and maintenance of the cyber security awareness training program.

Control: ISM-0735; Revision: 3; Updated: Dec-22; Applicable: NC, OS, P, S, TS; Essential 8: N/A
The CISO oversees the development, implementation and maintenance of their organisation's cyber security awareness training program.

Further information

Further information on responding to cyber security incidents can be found in the 'Managing cyber security incidents' section of the *Guidelines for cyber security incidents*.

Further information on the development of a cyber security strategy can be found in the 'Development and maintenance of cyber security documentation' section of the *Guidelines for cyber security documentation*.

Further information on cyber supply chain risk management can be found in the 'Cyber supply chain risk management' section of the *Guidelines for procurement and outsourcing*.

Further information on the procurement of outsourced services can be found in the 'Managed services and cloud services' section of the *Guidelines for procurement and outsourcing*.

Further information on cyber security awareness training programs can be found in the 'Cyber security awareness training' section of the *Guidelines for personnel security*.

System owners

System ownership and oversight

System owners are responsible for ensuring the secure operation of their systems. However, system owners may delegate the day-to-day management and operation of their systems to system managers. It is recommended that system owners collaborate with their organisation's internal cyber security teams or engage external cyber security specialists to assist them with their cyber security responsibilities.

Control: ISM-1071; Revision: 1; Updated: Sep-18; Applicable: NC, OS, P, S, TS; Essential 8: N/A
Each system has a designated system owner.

Control: ISM-1525; Revision: 1; Updated: Jan-21; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners register each system with its authorising officer.

Protecting systems and their resources

Broadly, the risk management framework defined by the *Information security manual* has six steps: define the system, select security controls, implement security controls, assess security controls, authorise the system and monitor the system. System owners are responsible for the implementation of this six-step risk management framework for each of their systems.

Control: ISM-1633; Revision: 2; Updated: Mar-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners, in consultation with each system's authorising officer, determine the system boundary, business criticality, and security and resilience objectives for each system based on an assessment of the impact if it were to be compromised or attacked.

Control: ISM-1203; Revision: 1; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners, in consultation with each system's authorising officer, conduct a threat and risk assessment for each system.

Control: ISM-1634; Revision: 4; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners, in consultation with each system's authorising officer, select security controls for each system and tailor them to achieve desired security and resilience objectives.

Control: ISM-0009; Revision: 5; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners, in consultation with each system's authorising officer, identify any supplementary security controls required based upon the unique nature of each system, its operating environment and the organisation's risk tolerances.

Control: ISM-1635; Revision: 3; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners implement security controls for each system and its operating environment.

Control: ISM-1636; Revision: 4; Updated: Sep-26; Applicable: NC, OS, P, S; Essential 8: N/A
System owners, in consultation with each system's authorising officer, ensure security controls for each non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET system and its operating environment undergo a security control assessment by their organisation's own assessors or Infosec Registered Assessor Program (IRAP) assessors to determine if they have been implemented correctly and are operating as intended.

Control: ISM-1967; Revision: 2; Updated: Sep-26; Applicable: TS; Essential 8: N/A
System owners, in consultation with each system's authorising officer, ensure security controls for each TOP SECRET system and its operating environment, including each sensitive compartmented information system and its operating environment, undergo a security control assessment by ASD assessors (or their delegates) to determine if they have been implemented correctly and are operating as intended.

Control: ISM-0027; Revision: 6; Updated: Mar-26; Applicable: NC, OS, P, S; Essential 8: N/A
System owners obtain an authorisation to operate for each non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET system from its authorising officer.

Control: ISM-1968; Revision: 1; Updated: Mar-26; Applicable: TS; Essential 8: N/A
System owners obtain an authorisation to operate for each TOP SECRET system, including for each sensitive compartmented information system, from Director-General ASD (or their delegate).

Control: ISM-1526; Revision: 4; Updated: Sep-26; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners continuously monitor the security of each system, and manage associated cyber threats, security risks and security controls.

Control: ISM-2021; Revision: 0; Updated: Jun-25; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners implement and maintain data minimisation practices for each of their systems.

Annual reporting of system security status

Annual reporting by system owners on the security status of their systems to their authorising officer can assist the authorising officer in maintaining awareness of the security posture of systems within their organisation.

Control: ISM-1587; Revision: 0; Updated: Aug-20; Applicable: NC, OS, P, S, TS; Essential 8: N/A
System owners report the security status of each system to its authorising officer at least annually.

Further information

Further information on using the *Information security manual*'s six-step risk management framework can be found in the 'Applying a risk-based approach to cyber security' section of *Using the cyber security framework*.

Further information on the purpose of IRAP is available from ASD.

Further information on conducting security assessment activities as part of continuously monitoring the security of systems can be found in the 'Security assessments' section of the *Guidelines for security assurance*.

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

© Commonwealth of Australia 2026

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license (https://creativecommons.org/licenses/by/4.0/).

For the avoidance of doubt, this means this license only applies to material as set out in this document.

The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license (https://creativecommons.org/licenses/by/4.0/legalcode.en).

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