Information security manual

Last updated: March 2025

Guidelines for cybersecurity roles

Board of directors and executive committee

Embedding cybersecurity

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

Control: ISM-1997; Revision: 0; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The board of directors or executive committee defines clear roles and responsibilities for cybersecurity both within the board of directors or executive committee and broadly within their organisation.

Control: ISM-1998; Revision: 0; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The board of directors or executive committee ensures that cybersecurity is integrated throughout all business functions within their organisation.

Control: ISM-1999; Revision: 0; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The board of directors or executive committee ensures the cybersecurity strategy for their organisation is aligned with the overarching strategic direction and business strategy for their organisation.

Control: ISM-2000; Revision: 0; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The board of directors or executive committee seeks regular briefings or reporting on the cybersecurity posture of their organisation, as well as the threat environment in which they operate, from internal and external subject matter experts.

Championing a positive cybersecurity culture

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

Control: ISM-2001; Revision: 0; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The board of directors or executive committee champions a positive cybersecurity culture within their organisation, including through leading by example.

Building cybersecurity expertise

To assist with embedding cybersecurity throughout an organisation, it is important that the board of directors or executive committee maintains a sufficient level of cybersecurity 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 cybersecurity recruitment activities, retention rates for cybersecurity personnel, and cybersecurity skills and experience gaps for their organisation. Finally, the board of directors or executive committee should support the development of cybersecurity skills and experience for all personnel within their organisation.

Control: ISM-2002; Revision: 0; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The board of directors or executive committee maintains a sufficient level of cybersecurity literacy to fulfil both their fiduciary duties and any legislative or regulatory obligations.

Control: ISM-2003; Revision: 0; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The board of directors or executive committee maintains awareness of key cybersecurity recruitment activities, retention rates for cybersecurity personnel, and cybersecurity skills and experience gaps within their organisation.

Control: ISM-2004; Revision: 0; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The board of directors or executive committee supports the development of cybersecurity skills and experience for all personnel via internal and external cybersecurity awareness raising and training opportunities.

Identifying critical business assets

In order 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, applications and data, including 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.

Control: ISM-2005; Revision: 0; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
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.

Planning for major cybersecurity incidents

In order 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 cybersecurity incidents, including by participating in exercises, and understand their duties in relation to such cybersecurity incidents.

Control: ISM-2006; Revision: 0; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The board of directors or executive committee plans for major cybersecurity incidents, including by participating in exercises, and understand their duties in relation to such cybersecurity incidents.

Further information

Further information on how the board of directors or executive committee can protect themselves from cyberthreats can be found in the Australian Signals Directorate's (ASD) *Practical cybersecurity 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 *Questions for the board of directors to ask about cybersecurity* and *Ten things to know about data security* publications.

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

Further information on cybersecurity 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 cybersecurity 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

Breadth of responsibilities

The role of the chief information security officer (CISO) within an organisation should extend to information technology and operational technology. However, where appropriate and practical to do so, responsibility for operational technology cybersecurity may be delegated by the CISO.

Within this section, the breadth of responsibilities for information technology and operational technology are collectively referenced under the banner of cybersecurity.

Required skills and experience

The role of the CISO requires a combination of technical and soft skills, such as business acumen, leadership, communications and relationship building. Additionally, a CISO should adopt a continuous approach to learning and up-skilling in order to maintain pace with the cyberthreat landscape and new technologies. It is expected that a CISO show innovation and imagination in conceiving and delivering cybersecurity strategies for their organisation.

Providing cybersecurity leadership and guidance

To provide cybersecurity leadership and guidance within an organisation (for information technology and operational technology), it is important that the organisation appoints a CISO.

Control: ISM-0714; Revision: 7; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
A CISO is appointed to provide cybersecurity leadership and guidance for their organisation (covering information technology and operational technology).

Overseeing the cybersecurity program

The CISO within an organisation is responsible for overseeing their organisation's cybersecurity program and ensuring compliance with cybersecurity 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: 2; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The CISO oversees their organisation's cybersecurity program and ensures their organisation's compliance with cybersecurity policy, standards, regulations and legislation.

Control: ISM-1617; Revision: 1; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The CISO regularly reviews and updates their organisation's cybersecurity program to ensure its relevance in addressing cyberthreats and harnessing business and cybersecurity opportunities.

Control: ISM-1966; Revision: 0; Updated: Dec-24; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The CISO develops, implements, maintains and verifies on a regular basis a register of systems used by their organisation.

Control: ISM-0724; Revision: 3; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The CISO implements cybersecurity measurement metrics and key performance indicators for their organisation.

Coordinating cybersecurity

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

Control: ISM-0725; Revision: 4; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The CISO coordinates cybersecurity and business alignment through a cybersecurity steering committee or advisory board, comprising of key cybersecurity and business executives, which meets formally and on a regular basis.

Control: ISM-0726; Revision: 3; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The CISO coordinates security risk management activities between cybersecurity and business teams.

Reporting on cybersecurity

The CISO is responsible for reporting cybersecurity 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 cybersecurity uplift activities
- any recent cybersecurity incidents
- expected returns on cybersecurity investments.

Reporting on cybersecurity 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 is able to translate security risks into operational risks for their organisation, including financial and legal risks, in order to enable more holistic conversations about their organisation's risks.

Control: ISM-0718; Revision: 5; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The CISO regularly reports directly to their organisation's board of directors or executive committee on cybersecurity matters.

Control: ISM-1918; Revision: 1; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The CISO regularly reports directly to their organisation's audit, risk and compliance committee (or equivalent) on cybersecurity matters.

Overseeing cybersecurity incident response activities

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

The CISO is also responsible for overseeing their organisation's response to cybersecurity incidents, including how internal teams respond and communicate with each other during cybersecurity incidents. In the event of a major cybersecurity 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: 3; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The CISO is fully aware of all cybersecurity incidents within their organisation.

Control: ISM-1618; Revision: 1; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The CISO oversees their organisation's response to cybersecurity 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; Applicability: NC, OS, P, S, TS; Essential Eight: 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 cybersecurity vision and strategy

To assist in facilitating cybersecurity 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 cybersecurity leader and continually communicate the cybersecurity vision and strategy for their organisation. In doing so, a cybersecurity 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: 4; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The CISO oversees the development, implementation and maintenance of a cybersecurity communications strategy to assist in communicating the cybersecurity 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 ongoing management. As supplier relationships come with additional security risks, the CISO should assist personnel with assessing cyber supply chain risks and understand the security impacts of entering into contracts with suppliers.

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

Receiving and managing a dedicated cybersecurity budget

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

Control: ISM-0732; Revision: 3; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The CISO receives and manages a dedicated cybersecurity budget for their organisation.

Overseeing cybersecurity personnel

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

Control: ISM-0717; Revision: 3; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The CISO oversees the management of cybersecurity personnel within their organisation.

Overseeing cybersecurity awareness raising

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

Control: ISM-0735; Revision: 4; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
The CISO oversees the development, implementation and maintenance of their organisation's cybersecurity awareness training program.

Further information

Further information on responding to cybersecurity incidents can be found in the managing cybersecurity incidents section of the *Guidelines for cybersecurity incidents*.

Further information on the development of a cybersecurity strategy can be found in the development and maintenance of cybersecurity documentation section of the *Guidelines for cybersecurity 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 cybersecurity awareness training programs can be found in the cybersecurity 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.

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

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

Protecting systems and their resources

Broadly, the risk management framework used by the *Information security manual* has six steps: define the system, select controls, implement controls, assess 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: 1; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
System owners, in consultation with each system's authorising officer, determine the system boundary, business criticality and security objectives for each system based on an assessment of the impact if it were to be compromised.

Control: ISM-1634; Revision: 2; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
System owners, in consultation with each system's authorising officer, select controls for each system and tailor them to achieve desired security objectives.

Control: ISM-1635; Revision: 2; Updated: Jun-22; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
System owners implement controls for each system and its operating environment.

Control: ISM-1636; Revision: 3; Updated: Mar-25; Applicability: NC, OS, P, S; Essential Eight: N/A
System owners, in consultation with each system's authorising officer, ensure controls for each non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET system and its operating environment undergo a security 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: 1; Updated: Mar-25; Applicability: TS; Essential Eight: N/A
System owners, in consultation with each system's authorising officer, ensure controls for each TOP SECRET system and its operating environment, including each sensitive compartmented information system and its operating environment, undergo a security assessment by ASD assessors (or their delegates) to determine if they have been implemented correctly and are operating as intended.

Control: ISM-0027; Revision: 5; Updated: Dec-24; Applicability: NC, OS, P, S; Essential Eight: N/A
System owners obtain authorisation to operate each non-classified, OFFICIAL: Sensitive, PROTECTED and SECRET system from its authorising officer based on the acceptance of the security risks associated with its operation.

Control: ISM-1968; Revision: 0; Updated: Dec-24; Applicability: TS; Essential Eight: N/A
System owners obtain authorisation to operate each TOP SECRET system, including each sensitive compartmented information system, from Director-General ASD (or their delegate) based on the acceptance of the security risks associated with its operation.

Control: ISM-1526; Revision: 3; Updated: Mar-25; Applicability: NC, OS, P, S, TS; Essential Eight: N/A
System owners monitor each system, and associated cyberthreats, security risks and controls, on an ongoing basis.

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; Applicability: NC, OS, P, S, TS; Essential Eight: 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 cybersecurity section of *Using the Information security manual*.

Further information on the purpose of IRAP, and a list of current IRAP assessors, is available from ASD.

Further information on monitoring systems and their operating environments can be found in the event logging and monitoring section of the *Guidelines for system monitoring*.

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