Information Security Manual

Last updated: June 2024

Guidelines for Cyber Security Roles

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 cyber security 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 cyber security.

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 must adopt a continuous approach to learning and up-skilling in order to maintain pace with the cyber threat landscape and new technologies. It is expected that a CISO show innovation and imagination in conceiving and delivering cyber security strategies for their organisation.

Providing cyber security leadership and guidance

To provide cyber security 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: 6; Updated: Jun-24; Applicability: All; Essential Eight: N/A
A CISO is appointed to provide cyber security leadership and guidance for their organisation (covering information technology and operational technology).

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; Applicability: All; Essential Eight: 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; Applicability: All; Essential Eight: 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-0724; Revision: 2; Updated: Oct-20; Applicability: All; Essential Eight: 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 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: 3; Updated: Dec-21; Applicability: All; Essential Eight: N/A
The CISO coordinates cyber security and business alignment through a cyber security steering committee or advisory board, comprising of key cyber security and business executives, which meets formally and on a regular basis.

Control: ISM-0726; Revision: 2; Updated: Oct-20; Applicability: All; Essential Eight: 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 executive committee or board of directors, 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 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: 4; Updated: Jun-24; Applicability: All; Essential Eight: N/A
The CISO regularly reports directly to their organisation's executive committee or board of directors on cyber security matters.

Control: ISM-1918; Revision: 0; Updated: Jun-24; Applicability: All; Essential Eight: 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 is able to accurately report to their organisation's executive committee or board of directors 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; Applicability: All; Essential Eight: N/A
The CISO is fully aware of all cyber security incidents within their organisation.

Control: ISM-1618; Revision: 0; Updated: Oct-20; Applicability: All; Essential Eight: 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; Applicability: All; 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 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 continually 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; Applicability: All; Essential Eight: 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 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: All; Essential Eight: 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; Applicability: All; Essential Eight: 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 and provide them with adequate authority and resources to perform their duties.

Control: ISM-0717; Revision: 2; Updated: Oct-20; Applicability: All; Essential Eight: N/A
The CISO oversees the management of cyber security personnel within their organisation.

Overseeing cyber security awareness raising

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; Applicability: All; Essential Eight: 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 security documentation section of the *Guidelines for 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.

Control: ISM-1071; Revision: 1; Updated: Sep-18; Applicability: All; Essential Eight: N/A
Each system has a designated system owner.

Control: ISM-1525; Revision: 1; Updated: Jan-21; Applicability: All; 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: 0; Updated: Jan-21; Applicability: All; Essential Eight: N/A
System owners determine the type, value and security objectives for each system based on an assessment of the impact if it were to be compromised.

Control: ISM-1634; Revision: 1; Updated: Jun-22; Applicability: All; Essential Eight: N/A
System owners select controls for each system and tailor them to achieve desired security objectives.

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

Control: ISM-1636; Revision: 1; Updated: Jun-22; Applicability: All; Essential Eight: N/A
System owners ensure controls for each system and its operating environment are assessed to determine if they have been implemented correctly and are operating as intended.

Control: ISM-0027; Revision: 4; Updated: Jan-21; Applicability: All; Essential Eight: N/A
System owners obtain authorisation to operate each system from its authorising officer based on the acceptance of the security risks associated with its operation.

Control: ISM-1526; Revision: 2; Updated: Jun-22; Applicability: All; Essential Eight: N/A
System owners monitor each system, and associated cyber threats, 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: All; 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 cyber security section of *Using the Information Security Manual*.

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*.

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

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

Australian Government

Australian Signals Directorate