Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JUNE 2021

Guidelines for Cyber Security Roles

Chief Information Security Officer

Required skills and experience

The role of the Chief Information Security Officer (CISO) requires a combination of technical and soft skills, such as business acumen, leadership, communications and relationship building. Additionally, CISOs 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 CISOs show innovation and imagination in conceiving and delivering cyber security strategies for their organisations.

Providing cyber security leadership and guidance

To provide cyber security leadership and guidance within organisations, it is important that each organisation appoints a CISO.

Security Control: 0714; Revision: 5; Updated: Oct-20; Applicability: O, P, S, TS
A CISO is appointed to provide cyber security leadership and guidance for their organisation.

Overseeing the cyber security program

The CISO within an organisation is typically responsible for providing strategic-level guidance for 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.

Security Control: 1478; Revision: 1; Updated: Oct-20; Applicability: O, P, S, TS
The CISO oversees their organisation's cyber security program and ensures their organisation's compliance with cyber security policy, standards, regulations and legislation.

Security Control: 1617; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
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.

Security Control: 0724; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
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 measures when planning new business projects. Additionally, as the CISO is responsible for the development of the strategic-level cyber security program, they are best placed to advise projects on the strategic direction of cyber security.

Security Control: 0725; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO coordinates cyber security and business alignment through a cyber security steering committee or advisory board, comprising of key business and ICT executives, which meets formally and on a regular basis.

Security Control: 0726; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO coordinates security risk management activities between cyber security and business teams.

Reporting on cyber security

The CISO is responsible for directly reporting cyber security matters to their organisation's senior executive and/or Board. 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 the organisation's security risks.

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

Security Control: 0718; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO reports directly to their organisation's senior executive and/or Board on cyber security matters.

Overseeing incident response activities

To ensure the CISO is able to accurately report to their organisation's senior executive and/or Board 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 an incident. 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.

Security Control: 0733; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO is fully aware of all cyber security incidents within their organisation.

Security Control: 1618; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
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 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.

Security Control: 0734; Revision: 3; Updated: Jun-21; Applicability: O, P, S, TS
The CISO contributes to the development 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.

Developing a cyber security communications strategy

To facilitate broad security cultural change across their organisation, the CISO should act as a thought leader continually communicating their strategy and vision. A communication strategy can be helpful in achieving this. Communications should be tailored to different parts of the organisation and be topical for the intended audience.

Security Control: 0720; Revision: 1; Updated: Oct-20; Applicability: O, P, S, TS
The CISO develops and maintains a cyber security communications strategy for their organisation.

Working with suppliers and service providers

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

Security Control: 0731; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO oversees cyber supply chain risk management activities for their organisation.

Managing a dedicated cyber security budget

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.

Security Control: 0732; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO 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 in order to ensure that sufficient resources are in place to perform cyber security functions. CISOs should delegate relevant tasks to cyber security managers and other personnel as required and provide them with adequate authority and resources to perform their duties.

Security Control: 0717; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
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 posture of their organisation, a cyber security awareness training program should be developed. As the CISO is responsible for cyber security within their organisation, they should oversee the development and operation of the program.

Security Control: 0735; Revision: 2; Updated: Oct-20; Applicability: O, P, S, TS
The CISO oversees the development and operation of their organisation's cyber security awareness training program.

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.

Security Control: 1071; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Each system has a designated system owner.

Security Control: 1525; Revision: 1; Updated: Jan-21; Applicability: O, P, S, TS
System owners register each system with its authorising officer.

Protecting systems and their resources

Broadly, the risk management framework used by the ***Australian Government 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.

Security Control: 1633; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS
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.

Security Control: 1634; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS
System owners select security controls for each system and tailor them to achieve desired security objectives.

Security Control: 1635; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS
System owners implement identified security controls within each system and its operating environment.

Security Control: 1636; Revision: 0; Updated: Jan-21; Applicability: O, P, S, TS
System owners ensure security controls for each system and its operating environment are assessed to determine if they have been implemented correctly and are operating as intended.

Security Control: 0027; Revision: 4; Updated: Jan-21; Applicability: O, P, S, TS
System owners obtain authorisation to operate each system from its authorising officer based on the acceptance of the security risks associated with its operation.

Security Control: 1526; Revision: 1; Updated: Jan-21; Applicability: O, P, S, TS
System owners monitor each system, and associated cyber threats, security risks and security controls, on an ongoing basis.

Annual reporting of system security status

Annual reporting on the security status of their systems to their authorising officers (e.g. by providing outcomes of any vulnerability scans and penetration tests) can assist authorising officers in maintaining awareness of the security posture of systems.

Security Control: 1587; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
System owners report the security status of each system to its authorising officer at least annually.

Further information

Further information on using the six step risk management framework can be found in ***Using the Australian Government Information Security Manual***.

Further information on monitoring systems and their operating environments can be found in the ***Guidelines for System Monitoring***.