Guidelines for cyber security roles

**Chief Information Security Officer**

**Cyber security leadership**

To provide cyber security leadership within organisations, it is important that each organisation appoints a Chief Information Security Officer (CISO).

*Security Control: 0714; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Must*

A CISO is appointed to provide cyber security leadership for their organisation.

**Responsibilities**

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, or report to, a Chief Security Officer (CSO) who is responsible for the full breadth of security within their organisation.

*Security Control: 1478; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS; Priority: Should*

The CISO provides strategic-level guidance for their organisation’s cyber security program and ensures their organisation’s compliance with cyber security policy, standards, regulations and legislation.

**Further information**

Further information on the duties of the CISO can be found in the *Guidelines for authorising systems*.

**System owners**

**System ownership**

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; Priority: Must*

Each system has a designated system owner.

**Responsibilities**

System owners are responsible for obtaining authorisation to operate each of their systems.
System owners register each system with the system’s authorising officer.

System owners obtain authorisation to operate each system from the system’s authorising officer.

System owners monitor security risks and the effectiveness of security controls for each system.

Further information

Further information on authorising officers and obtaining authorisation to operate systems can be found in the Guidelines for authorising systems.

Further information on change management processes can be found in the Change management section of the Guidelines for system management.

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