3.4. System Owners

Objective

3.4.1. All systems are allocated a **system owner** who has responsibility for the overall operation, including obtaining and maintaining any certification and accreditation, of the allocated system(s).

Context

Scope

3.4.2. This section covers the role that system owners undertake with respect to information security.

3.4.3. System owners are responsible for the overall operation of the system, including any outsourced services such as support, telecommunications and cloud.

3.4.4. System owners MUST ensure their systems are certified and accredited to meet their agency's operational requirements and that this status in maintained.

Assertions in Certification and Accreditation

3.4.5. Originating in financial auditing, assertions are now widely used as the basis for assurance processes covering a wide range of business activities and the related technology.

3.4.6. Assertions are formal statements by management or system owners. They are claims on the completeness, accuracy and validity of events, presentations, disclosure, transactions and related assurance, risk and governance aspects of certification and accreditation.

3.4.7. It is the responsibility of the management (or system owner) to prepare and validate assertions relating to the governance, assurance and security of information systems, in accordance with national policy and related standards.

3.4.8. When such assertions are made it means management (or system owners) have presented and disclosed information appropriately giving a true, fair and balanced view of the activities. In preparing assertions, implicit and explicit claims are made on the validity and completeness of the assertions.

3.4.9. Assertions are typically characterised as follows:

Transactions and events

- Occurrence — the activities recorded have actually taken place.
- Completeness — all aspects are properly recorded.
- Accuracy — the assets and activities are accurately allocated and recorded.
- Cutoff — the activities have been recorded in the correct time period.
- Classifications — are accurate and appropriate.

Position on project completion

- Existence — assets, liabilities and equity balances exist.
- Rights and Obligations — the entity legally controls rights to its assets and its liabilities and accurately records obligations.
- Completeness — all aspects are properly recorded.
- Valuation and Allocation — costs and assets appropriately valued and allocated.

Presentation and disclosure

- Occurrence — the events and implementations have actually occurred.
- Rights and Obligations — contracts, licences, support and supply agreements
- Completeness — all disclosures have been included in the statements.
- Classification — statements are clear and appropriately presented.
- Accuracy and Valuation — information is disclosed at the appropriate amounts.

Rationale & Controls

Requirement for system owners

3.4.10.R.01. **Rationale**

The system owner is responsible for the overall operation of the system, including any directly related support or outsourced service such as cloud. They may delegate the day-to-day management and operation of the system to a system manager or managers.

3.4.10.R.02. **Rationale**

All systems should have a system owner in order to ensure IT governance processes are followed and that business requirements are met.

3.4.10.R.03. **Rationale**

It is strongly recommended that a system owner be a member of the Senior Executive Team or in an equivalent management position, however this does not imply that the system manager(s) should also be at such a level.

3.4.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:442]

Each system MUST have a system owner who is responsible for the operation and maintenance of the system.

3.4.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:443]

System owners SHOULD be a member of the Senior Executive Team or an equivalent management position, for large or critical agency systems.

Accreditation responsibilities

3.4.11.R.01. **Rationale**

The system owner is responsible for the operation of their system and as such they need to ensure that systems are accredited to meet the agency's operational requirements. If modifications are undertaken to a system the system owner will need to ensure that the changes are undertaken in an appropriate manner, documented adequately and that any necessary reaccreditation activities are completed.

3.4.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:446]

System owners MUST obtain and maintain accreditation of their system(s).

Documentation responsibilities

3.4.12.R.01. **Rationale**

The system owner is responsible for ensuring the development, maintenance and implementation of Systems Information Security documentation, in particular the Security Risk Management Plans (SRMPs), System Security Plans (SSPs) and Standard Operating Procedures (SOPs).

3.4.12.R.02. **Rationale**

The system owner should involve security personnel in the process of developing, redeveloping or updating Systems Information Security documentation, to ensure that a holistic approach to information security is mapped to the system owner's understanding of security risks for their specific system. Information security documentation is detailed in Chapter 5 - Information Security documentation. Refer also to Chapter 4 - System Certification and Accreditation.

3.4.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:449]

System owners MUST ensure the development, maintenance and implementation of complete, accurate and up to date Information Security documentation for systems under their ownership. Such actions MUST be documented.

3.4.12.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:450]

System Owners MUST involve the ITSM in the redevelopment and updates of the Information Security documentation.