3.3. Information Technology Security Managers

Objective

3.3.1. Information Technology Security Managers (ITSM) provide information security leadership and management within their agency.

Context

Scope

3.3.2. This section covers the role of an ITSM with respect to information security within an agency.

Information technology security managers

3.3.3. ITSMs are executives within an agency that act as a conduit between the strategic directions provided by the CISO and the technical efforts of systems administrators. The main area of responsibility of an ITSM is that of the administrative and process controls relating to information security within the agency.

Rationale & Controls

Requirement for ITSMs

3.3.4.R.01. **Rationale**

When agencies outsource their ICT services, ITSMs should be independent of any company providing ICT services. This will prevent any conflict of interest for an ITSM in conducting their duties.

3.3.4.R.02. **Rationale**

Ensure that the agency has a point of presence at sites to assist with monitoring information security for systems and responding to any information security incidents.

3.3.4.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:367]

Agencies MUST appoint at least one ITSM within their agency.

3.3.4.C.02. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:368]

ITSMs MUST be:

- cleared for access to all classified information processed by the agency's systems; and
- able to be briefed into any compartmented information on the agency's systems.

3.3.4.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:369]

Where an agency is spread across a number of geographical sites, it is recommended that the agency SHOULD appoint a local ITSM at each major site.

3.3.4.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:370]

The ITSM role SHOULD be undertaken by personnel with an appropriate level of authority and training based on the size of the agency or their area of responsibility within the agency.

3.3.4.C.05. **Control System Classifications(s): All Classifications; Compliance: Should Not** [CID:371]

ITSMs SHOULD NOT have additional responsibilities beyond those needed to fulfil the role as outlined within this manual.

Responsibilities – Security programs

3.3.5.R.01.

Rationale

As ITSMs undertake operational management of information security within an agency they can provide valuable input to the development of the information security program by the CISO.

3.3.5.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:375]

ITSMs SHOULD work with the CISO to develop an information security program within the agency.

3.3.5.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:376]

ITSMs SHOULD undertake and manage projects to address identified security risks.

Responsibilities – Working with ICT projects

3.3.6.R.01. **Rationale**

As ITSMs have knowledge of all aspects of information security they are best placed to work with ICT projects within the agency to identify and incorporate appropriate information security measures.

3.3.6.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:379]

ITSMs MUST be responsible for assisting system owners to obtain and maintain the accreditation of their systems.

3.3.6.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:380]

ITSMs SHOULD identify systems that require security measures and assist in the selection of appropriate information security measures for such systems.

3.3.6.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:381]

ITSMs SHOULD consult with ICT project personnel to ensure that information security is included in the evaluation, selection, installation, configuration and operation of IT equipment and software.

3.3.6.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:382]

ITSMs SHOULD work with agency enterprise architecture teams to ensure that security risk assessments are incorporated into system architectures and to identify, evaluate and select information security solutions to meet the agency's security objectives.

3.3.6.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:384]

ITSMs SHOULD be included in the agency's change management and change control processes to ensure that risks are properly identified and controls are properly applied to manage those risks.

3.3.6.C.06. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:385]

ITSMs SHOULD notify the Accreditation Authority of any significant change that may affect the accreditation of that system.

Responsibilities – Working with vendors

3.3.7.R.01. **Rationale**

The CISO will coordinate the use of external information security resources to the agency, whilst ITSMs will be responsible for establishing contracts and service-level agreements on behalf of the CISO.

3.3.7.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:388]

ITSMs SHOULD liaise with vendors and agency purchasing and legal areas to establish mutually acceptable information security contracts and service-level agreements.

Responsibilities – Implementing security

3.3.8.R.01. **Rationale**

The CISO will set the strategic direction for information security within the agency, whereas ITSMs are responsible for managing the implementation of information security measures within the agency.

3.3.8.C.01. **Control System Classifications(s): All Classifications; Compliance: Must** [CID:391]

ITSMs MUST be responsible for ensuring the development, maintenance, updating and implementation of Security Risk Management Plans (SRMPs), Systems Security Plans (SSP) and any Standard Operating Procedures (SOPs) for all agency systems.

3.3.8.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:392]

ITSMs SHOULD conduct security risk assessments on the implementation of new or updated IT equipment or software in the existing environment and develop treatment strategies if necessary.

3.3.8.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:393]

ITSMs SHOULD select and coordinate the implementation of controls to support and enforce information security policies.

3.3.8.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:394]

ITSMs SHOULD provide leadership and direction for the integration of information security strategies and architecture with agency business and ICT strategies and architecture.

3.3.8.C.05. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:395]

ITSMs SHOULD provide technical and managerial expertise for the administration of information security management tools.

Responsibilities – Budgeting

3.3.9.R.01. **Rationale**

As ITSMs are responsible for the operational management of information security projects and functions within their agency, they will be aware of their funding requirements and can assist the CISO to develop information security budget projections and resource allocations.

3.3.9.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:398]

ITSMs SHOULD work with the CISO to develop information security budget projections and resource allocations based on short-term and long-term goals and objectives.

Responsibilities – Reporting

3.3.10.R.01. **Rationale**

To ensure the CISO remains aware of all information security issues within their agency, and can brief their agency head when necessary, ITSMs will need to provide regular reports on policy developments, proposed system changes and enhancements, information security incidents and other areas of particular concern to the CISO.

3.3.10.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:401]

ITSMs SHOULD coordinate, measure and report on technical aspects of information security management.

3.3.10.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:402]

ITSMs SHOULD monitor and report on compliance with information security policies, as well as the enforcement of information security policies within the agency.

3.3.10.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:403]

ITSMs SHOULD provide regular reports on information security incidents and other areas of particular concern to the CISO.

3.3.10.C.04. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:404]

ITSMs SHOULD assess and report on threats, vulnerabilities, and residual security risks and recommend remedial actions.

Responsibilities – Auditing

3.3.11.R.01. **Rationale**

As system owners may not understand the results of audits against their systems ITSMs will need to assist them in understanding and responding to reported audit failures. ITSM's should also refer to 5.8 Independent Assurance Reports.

3.3.11.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:407]

ITSMs SHOULD assist system owners and security personnel in understanding and responding to audit failures reported by auditors.

Responsibilities – Disaster recovery

3.3.12.R.01. **Rationale**

Whilst the CISO will coordinate the development of disaster recovery policies and standards within the agency, ITSMs will need to guide the selection of appropriate strategies to achieve the direction set by the CISO.

3.3.12.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:410]

ITSMs SHOULD assist and guide the disaster recovery planning team in the selection of recovery strategies and the development, testing and maintenance of disaster recovery plans.

Responsibilities – Training

3.3.13.R.01. **Rationale**

The CISO will oversee the development and operation of information security awareness and training programs within the agency. ITSMs will arrange delivery of that training to personnel within the agency.

3.3.13.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:413]

ITSMs SHOULD provide or arrange for the provision of information security awareness and training for all agency personnel.

3.3.13.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:414]

ITSMs SHOULD develop technical information materials and workshops on information security trends, threats, good practices and control mechanisms as appropriate.

Responsibilities – Providing security knowledge

3.3.14.R.01. **Rationale**

ITSMs will often have an extensive knowledge of information security topics and can provide advice for the information security steering committee, change management committee and other agency and inter-agency committees.

3.3.14.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:418]

ITSMs SHOULD maintain a current and up-to-date security knowledge base comprising of a technical reference library, security advisories and alerts, information on information security trends and practices, and relevant laws, regulations, standards and guidelines.

3.3.14.C.02. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:419]

ITSMs SHOULD provide expert guidance on security matters for ICT projects.

3.3.14.C.03. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:420]

ITSMs SHOULD provide technical advice for the information security steering committee, change management committee and other agency and inter-agency committees as required.

Responsibilities

3.3.15.R.01. **Rationale**

ITSMs are generally considered the information security experts within an agency and as such their contribution to improving the information security of systems, providing input to agency ICT projects, assisting other security personnel within the agency, contributing to information security training and responding to information security incidents is a core aspect of their work.

3.3.15.R.02. **Rationale**

An ITSM is likely to have the most up to date and accurate understanding of the threat environment relating to systems. As such, it is essential that this information is passed to system owners to ensure that it is considered during accreditation activities.

3.3.15.C.01. **Control System Classifications(s): All Classifications; Compliance: Should** [CID:424]

The ITSM SHOULD keep the CISO and system owners informed with up-to-date information on current threats.