SACSF Guideline - Information technology security adviser (ITSA) role and responsibilities

Background

All agencies will appoint an information technology security adviser (ITSA), as directed by Premier and Cabinet Circular PC030.

Guidance

This guideline describes the role, responsibilities and required capabilities of the ITSA, including how to appoint a person to the role.

Role of the ITSA

The ITSA provides support and advice to senior management and agency staff on cyber security. This is to make sure digital information that is stored, processed or communicated by the agency's information systems and services is secured.

The agency chief executive may ask the ITSA to fulfil the cyber security program owner responsibilities, or other functions, identified in the South Australian Cyber Security Framework (SACSF). This decision will be based on agency requirements.

The ITSA must maintain high levels of trust, integrity and responsibility. The ITSA will provide support and direct, independent and impartial advice to the agency security executive (ASE) and also work closely with the agency security adviser (ASA).

The ITSA will be DPC's main contact for ICT security matters. DPC will regularly advise and consult them in relation to threats to the state government's ICT infrastructure, systems and services.

Appointing an ITSA

The Chief Executive is accountable for appointing the ITSA however the Agency Security Executive can formally authorise the appointment of the ITSA and provide notification of the appointment to DPC Office for Cyber Security.

It is expected that agencies with more than 500 personnel dedicate 1 FTE to the ITSA role and the ITSA role is included in the job and person specification.

Requirements of an ITSA

Agencies should make sure that the person considered for the role of ITSA:

Is an SA Government employee

The position of ITSA must be held by an SA Government employee. It is recognised that an ITSA may not have extensive knowledge on all security issues and may seek guidance from external providers.

Has both broad business and technical knowledge

The ITSA must be able to provide advice on complex technological ICT systems and service security matters to executives and business owners. They will also need to communicate risks in a way that all personnel can understand.

Has broad knowledge of current ICT security practice

The ITSA must have detailed knowledge of agency-specific and South Australian Government protective security policies, principles and minimum standards. They must also be provided with opportunities to maintain this knowledge.

Has a security clearance at the required level

The ITSA will need a South Australian Government security clearance of at least 'Baseline' level. Their clearance must be appropriate for the information or systems they need to access to do their job. Further information on clearance levels is available from the Australian Government Security Vetting Agency.

Has relevant ICT experience

Personnel appointed to the ITSA position is expected to have experience in one or more of the following roles:

- Security
- Risk, Audit, Assurance or Compliance
- Governance
- Technical ICT.

Has no conflicting operational demands and responsibilities

The ITSA position must be able to offer independent and impartial advice without resourcing and financial constraints.

Responsibilities and competencies

Typical responsibilities and minimum skill requirements are described in the role statement for ITSAs.

Additional responsibilities

The ITSA may also need to:

- provide ICT security briefings and advice to agency personnel, including staff located or travelling overseas
- investigate and report cyber security incidents to DPC, and the ASA

- fulfil the cyber security program owner responsibilities, or other functions, identified in the SACSF. This decision will be based on the individual requirements of the agency and the agency chief executive
- attend SA government ITSA briefings, events and forums
- assist the Watchdesk during a Cyber Crisis as detailed in PC042 - Cyber Security Incident Management.

Additional competencies

The ITSA should also have, or be given training to develop competency in the following areas:

- communication and business management skills
- comprehensive knowledge of the principles, policy statements and expectations which govern the security of government ICT systems
- awareness of technological controls and complementary security requirements contained in internationally recognised frameworks, for example:
    - the Australian Government Information Security Manual (ISM)
    - ISO 27001/27002
    - NIST
- measures to detect and manage cyber security incidents and preserve evidence for security investigations.

Reference, links and additional information

- South Australian Cyber Security Framework
- PC030 South Australian Protective Security Framework
- Australian Government Protective Security Policy Framework (PSPF)

Document Control

ID	SACSF/5.0
Version	V1.0
Classification/DLM	OFFICIAL
Compliance	Discretionary
Original authorisation date	November 2019
Last approval date	November 2019
Next review date	November 2020