DPC/R1.0

GOVERNMENT RULING ON CYBER SECURITY

ISMF Ruling 1 - Security management requirements for critical information and communication technology

Background

This ruling is issued for application of the South Australian Government Information Security Management Framework (ISMF) to critical information communications technology (ICT). It is an official interpretive statement applicable to South Australian Government agencies and suppliers whose contractual requirements include it.

The ISMF applies to all Official Information, and all information of which the South Australian Government or any of its Agencies has custody, where that information is processed, stored or communicated by ICT equipment.

This ruling should be read in conjunction with ISMF Guideline 37a.

Purpose

What this ruling is about:

1. It defines the criterion that constitutes State Government Critical ICT Infrastructure (SGCII)
2. It describes how SGCII shall be registered
3. It explains how the standards and provisions of the ISMF shall be applied to information infrastructure classified as State Government Critical ICT Infrastructure
4. It explains how the waiver (exemption) provision of the ISMF applies to SGCII
5. It reminds agencies of the timeline for the establishment of an Information Security Management System (ISMS) and corresponding statement of applicability that encompasses SGCII.

Ruling

Agencies are responsible for providing the Department of the Premier and Cabinet (DPC) with information related to the Critical Services they provide, including any ICT that underpins it. The desired outcome of the collected data is a single information resource that describes the relationships between the services delivered by the Government, the related ICT services and the underpinning ICT infrastructure.

This single information resource will take the form of a SGCII Register managed by DPC.

What constitutes State Government Critical ICT Infrastructure?

State Government Critical ICT Infrastructure (SGCII)

SGCII is defined as ICT infrastructure upon which '*Critical Services'* are delivered to the community. If the confidentiality, integrity or availability of this ICT infrastructure is lost then it could significantly impact on the social, or economic well-being of the State, the government, commercial entities or members of the public.

Critical Services

Critical Services are those services that, if compromised, would result in significant damage to the physical, social or economic wellbeing of the State. Critical Services are not typically ICT services, they are services that an agency delivers to the community on behalf of the Government.

Critical Services can be categorised as either Essential or Important:

Essential Services

- Essential Services are those services (whether provided by a public or private undertaking) without which the safety, health or welfare of the community or a section of the community would be endangered or seriously prejudiced[1].

  Essential Services are directly related to:

  - continuity of executive government
  - directly combating identified threats
  - physical survival of the community

Important Services

- Important Services are those services that are directly related to the social, physical or economic safety and security of the State.

Registration of State Government Critical ICT Infrastructure

Responsible Parties are to identify any SGCII in their agency and inform DPC for recording in the SGCII Register. Responsible Parties should describe the relationships between the Critical Services delivered by the agency, their supporting ICT services and underpinning ICT infrastructure.

Responsible parties shall review their submission annually or on an event driven basis and inform DPC of amendments. The Agency Chief Executive, or appropriate delegate (e.g. Agency Security Executive), should sign off on any agency asset being registered as SGCII.

Application of the standards and provisions of the ISMF to SGCII

The ISMF identifies the minimum controls required by all Agencies and Suppliers regardless of the scope of their ISMS implementation(s). This control set effectively establishes the cyber security baseline for across government ICT services and operations.

In addition to the baseline cyber security control set, the standards and provisions of ISMF version 3, in its entirety will apply to SGCII. Application of the additional standards and provisions will be selected based upon the outcome of a risk assessment.

[1] South Australian *Essential Services Act, 1981*

Waiver of the ISMF provisions for SGCII

ISMF version 3 introduces the ability for an Agency to seek an exemption from select standards or provisions issued under the ISMF.

Information infrastructure classified as SGCII is **not** eligible for an exemption or waiver using the DPC exemptions process. Instead, any Agency seeking an exemption for any assets classified as SGCII should follow the waivers process listed in section 5.8 of the Protective Security Management Framework.

Timeline for the establishment of an ISMS

Agencies have until 30 June 2013 to establish an ISMS and develop a statement of applicability for their operating environment that encompasses critical ICT information assets and associated activities. Agencies must have 100% of the ICT component of State Government Critical Infrastructure and business critical assets accounted for in their management system by this date.

For further information on the timeline refer to ISMF Guideline 1a – Transition Guidance for Agencies and Suppliers.

References, links and additional information

- Information Security Management Framework
- PC030 Protective Security Management Framework
- ISMF Guideline 37a – Critical Information and Communication Technology
- ISMF Guideline 1a – Transition Guidance for Agencies and Suppliers

Document Control

ID	DPC/R1.0 *previously DPC/R4.1*
Version	1.2
Classification/DLM	OFFICIAL
Compliance	Mandatory
Original authorisation date	June 2012
Last approval date	February 2019
Next review date	February 2020