# 11 Robust ICT systems

## A. Purpose

1. This policy describes how entities can safeguard information and communication technology (ICT) systems to support the secure and continuous delivery of government business. Robust ICT systems protect the confidentiality, integrity and availability of the information that entities process, store and communicate.

## B. Requirements

### B.1 Core requirement

***Each entity must ensure the secure operation of their ICT systems to safeguard information and the continuous delivery of government business by applying the Australian Government Information Security Manual's cyber security principles during all stages of the lifecycle of each system.***

### B.2 Supporting requirements

**Supporting requirements for robust ICT systems**

| # | Supporting requirements |
|---|---|
| **Requirement 1. Authorisation of ICT systems to operate** | Entities **must** only process, store or communicate information on ICT systems that the determining authority (or their delegate) has authorised to operate based on the acceptance of the residual security risks associated with its operation.<br><br>When establishing new ICT systems, or implementing improvements to existing systems, the decision to authorise (or reauthorise) an ICT system to operate **must** be based on the *Australian Government Information Security Manual*'s six step risk-based approach for cyber security. |
| **Requirement 2. Secure internet gateways** | Entities **must** protect internet-connected ICT systems, and the information they process, store or communicate, by implementing a secure internet gateway that meets Australian Signals Directorate requirements. |

## C. Guidance

### C.1 Secure ICT systems at all stages of their lifecycle

2. An ICT system is defined as the related set of hardware and software used to process, store or communicate information, and the governance framework in which it operates.
3. As mandated in the **core requirement**, entities must ensure the secure operation of each ICT system the entity operates or outsources, and manage the associated security risks during all stages of the lifecycle of the system. The phases of an ICT system's lifecycle are outlined in **Figure 1**.
4. This approach will improve both the trustworthiness and resilience of ICT systems (and associated components) that government relies on to protect information from compromise and ensure the secure and continuous delivery of Australian Government operations.

### C.1.1 Cyber security principles

5. Key to safeguarding ICT systems from cyber threats and achieving 'managing level' maturity with the **core requirement** is the effective implementation of the Australian Government Information Security Manual (ISM) cyber security principles. This approach includes identifying the key security risks to each ICT system and implementing appropriate and effective security controls from the ISM to manage the security risks identified for each ICT system.
6. The ISM's cyber security principles are grouped into four key activities:
   a. **Govern**: Identifying and managing security risks.
   b. **Protect**: Implementing security controls to reduce security risks.
   c. **Detect**: Detecting and understanding cyber security events.
   d. **Respond**: Responding to and recovering from cyber security incidents.
7. For advice on assessing the level of implementation of the ISM's cyber security principles, see the Australian Cyber Security Centre's (ACSC) maturity modelling advice for cyber security principles.
8. See PSPF policy 5: Reporting on security for information for further advice on 'managing level' maturity.

### C.1.2 Security considerations for new or existing ICT systems

9. When establishing new ICT systems, implementing improvements to current ICT systems or performing subsequent maintenance of existing systems, it is important that security is considered during the design of the system, rather than retrofitting security protections at a later time.[1]
10. Outlined below are the key security topics that may warrant consideration during the development of an ICT system or subsequent maintenance of existing systems. Ongoing consideration of these topics throughout the lifecycle of an ICT system is important to maintaining cyber security. Key security topics to consider are:
    a. **Cyber security roles**: Specific cyber security roles and titles (other than the Chief Security Officer, outlined in PSPF policy 2: Management structures and responsibilities) are not mandated under this policy. However, some entities may wish to appoint a Chief Information Security Officer (CISO) to support the CSO with managing cyber security in the entity. For guidance on other cyber security roles, including the CISO role and system owners, see the ISM's *Guidelines for Cyber Security Roles*.
    b. **Cyber security incident management**: Early detection of a cyber security incident and timely reporting to the entity's CSO or CISO is critical to expediting containment and recovery. PSPF policy 5: Reporting on security outlines requirements for reporting security incidents, including cyber security incidents. See also the ISM's *Guidelines for Cyber Security Incidents*.
    c. **Managing security risks when outsourcing**: Outsourcing can be a cost-effective option for providing information technology and cloud services, as well as potentially delivering a superior service. However, it can also affect an entity's security risk profile. For further guidance see Section **C.2.3** and the ISM's *Guidelines for Outsourcing*.
    d. **Security documentation**: Preparing relevant documentation supports implementing PSPF policy and ISM guidance. Preparing a security risk management plan is mandated in PSPF policy 3: Security planning and risk management. See also the ISM's *Guidelines for Security Documentation*.
    e. **Physical security**: Physical security requirements for ICT equipment and facilities are outlined in PSPF policies 15: Physical security for entity resources, and 16: Entity resources. For additional guidance on wireless devices in physically secure areas, see the ISM's *Guidelines for Physical Security*.
    f. **Personnel security**: As outlined in PSPF policy 2: Management structures and responsibilities, entities are required to ensure all personnel are provided with security awareness training. For further guidance on cyber security awareness training, see the ISM's *Guidelines for Personnel Security*.

[1] Given the potential inter-relationship between privacy and security issues, entities are encouraged to consider relevant Australian Privacy Principles in project conception and design. For information, see the OAIC's Guide to securing personal information.

g. **Access control**: Well-structured and robust ICT systems allow necessary access for personnel to undertake their work while protecting sensitive and classified information, intellectual property and personal information. PSPF policy 9: Access to information requires entities to control access to ICT systems, networks (including remote access), infrastructure and applications. See also the ISM's *Guidelines for Personnel Security*.

h. **Administrator privileges**: Restricting administrative privileges is one of the most effective ways to safeguard ICT systems. For policy and guidance on the restriction of administrative privileges, see PSPF policy 10: Safeguarding information from cyber threats. See also the ISM's *Guidelines for Personnel Security*.

i. **Communications infrastructure**: Infrastructure security includes good cable management and security regimes that help entities maintain the integrity and availability of communications infrastructure as well as the confidentially of information. For further guidance, see the ISM's *Guidelines for Communications Infrastructure*.

j. **Communications systems**: It is important to consider other types of devices and services that are attached to an ICT system. For example, telephone systems, video conferencing, internet protocol telephony and multifunctional devices. See the ISM's *Guidelines for Communications Security*.

k. **Product security**: It is important that entities gain assurance that products with a security function perform as claimed by vendors and provide the necessary measures to mitigate cyber threats. There are a number of methods to achieve assurance, including through formal and impartial evaluation, see the ISM's *Guidelines for Evaluated Products*. ASD performs limited product evaluations through the following programs:

    i. ASD Cryptographic Evaluation (ACE) program – for products used to protect PROTECTED information.

    ii. High Assurance Evaluation program – for products used to protect SECRET information (and above).

    iii. Australasian Information Security Evaluation Program (AISEP) – for product evaluations in accordance with the Common Criteria.

l. **ICT equipment management**: ICT equipment requires ongoing management to ensure the information it processes, stores or communicates remains protected in an appropriate manner. For guidance on ICT management, maintenance, repairs and sanitisation or disposal, see the ISM's *Guidelines for ICT Equipment*. See PSPF policy 15: Physical security for entity resources for guidance on disposal of an ICT system at the end of its life.

m. **Media security**: Implementing sound security practices when connecting, storing, transferring, sanitising, destroying or disposing of media plays a major role in reducing cyber threats and preventing the unauthorised disclosure of sensitive or classified data. Media security is particularly important when decommissioning an ICT system. PSPF policy 8: Sensitive and classified information provides guidance on the sanitisation or destruction of ICT equipment and media. See also the ISM's *Guidelines for ICT Equipment* and *Guidelines for Media*.

n. **System hardening**: Newer versions of operating systems often introduce improvements in security functionality over older versions. Using older versions of operating systems, especially those no longer supported by vendors, exposes entities to exploitation techniques that have since been mitigated in newer versions of operating systems. See the ISM's *Guidelines for System Hardening*.

o. **System administration**: Secure system administration allows an entity to be resilient in the face of targeted cyber intrusions by protecting administrator workstations and accounts from compromise, as well as making adversary movement throughout a network more difficult. See the ISM's *Guidelines for System Management*.

p. **Continuous system monitoring**: Continuous monitoring of an ICT system can assist in proactively identifying, prioritising and responding to security vulnerabilities and provide valuable information about exposure to cyber threats. Ongoing monitoring as a continuous improvement cycle is outlined in PSPF policy 4: Security maturity monitoring. See also the ISM's *Guidelines for Security Documentation* and *Guidelines for System Monitoring*.

q. **Software security**: It is important to implement and maintain measures to protect against software and database security vulnerabilities that may be used to undermine the integrity or availability of ICT systems or information. See the ISM's *Guidelines for Software Development* and *Guidelines for Database Systems*.

r. **Email management**: To guard against information compromise, PSPF policy 8: Sensitive and security classified information outlines the requirements to identify sensitive and security classified information, including emails, using the applicable protective marking. The Email Protective Marking Standard provides guidance for applying protective markings and, where relevant, information management markers, on emails exchanged in and between entities. See also the ISM's *Guidelines for Email*.

s. **Network management**: Network management practices and procedures assist in identifying and addressing network design or configuration vulnerabilities. It is important that network documentation accurately depicts the current state of a network. See the ISM's *Guidelines for Networking*.

t. **Cryptography**: Cryptography is primarily used to restrict access to information to authorised users. It provides confidentiality, integrity, authentication and nonrepudiation of information. Encryption protects the confidentiality of data by making it unreadable to unauthorised users. See the ISM's *Guidelines for Cryptography*.

u. **Gateway security**: Gateway security assists in mitigating security risks by securely managing data flows between different security domains, see the ISM's *Guidelines for Gateways*. This includes:

   i. deploying and configuring gateways to manage information flows (ingress and egress of traffic) across security boundaries between networks

   ii. implementing firewalls to protect against network-based intrusions

   iii. using diodes to protect against data spills and adversaries seeking to use information flows to intrude on or attack networks

   iv. allowing web access while protecting against the execution and spread of malicious software

   v. using content filtering techniques to reduce the risk of unauthorised or malicious content crossing a security boundary

   vi. sharing peripherals between ICT systems and ensuring unauthorised information does not pass between different security domains.

v. **Data transfers**: Implementing formal procedures can assist in ensuring that information transferred between ICT systems is done in a secure and auditable manner. See the ISM's *Guidelines for Data Transfers*.

## C.2 Authorisation of ICT systems to operate

11. **Requirement 1** mandates that all ICT systems require authorisation to operate to ensure that an appropriate level of security is being applied to the system and that residual security risks have been accepted by the relevant authority. This will provide confidence the ICT system meets security objectives, addresses known security vulnerabilities and remains secure. An impartial (and in some cases independent) security assessment can be a valuable tool in authorisation decisions.

12. The determining authorities for authorisation of ICT systems to operate, as required in **Requirement 1**, are outlined in Section **C.2.2** and **Table 1**.

13. Interconnection of ICT systems creates a potential vector for adversaries to target systems via third parties. As part of the security assessment and authorisation process, where ICT systems will be connected to other systems outside the entity's control, consider the security risks and what security protections are required between the systems. For example, interconnections with another entity's ICT systems, State and Territory systems, industry partner systems, or an international partners' systems. Before interconnection is established, it is important to share information on security risks to ensure any shared residual security risks are accepted by both entities.

14. ICT systems are required to be authorised to at least the sensitivity or classification of the information it will process. Refer to PSPF policy 8: Sensitive and classified information for guidance on protective markings and security classifications.

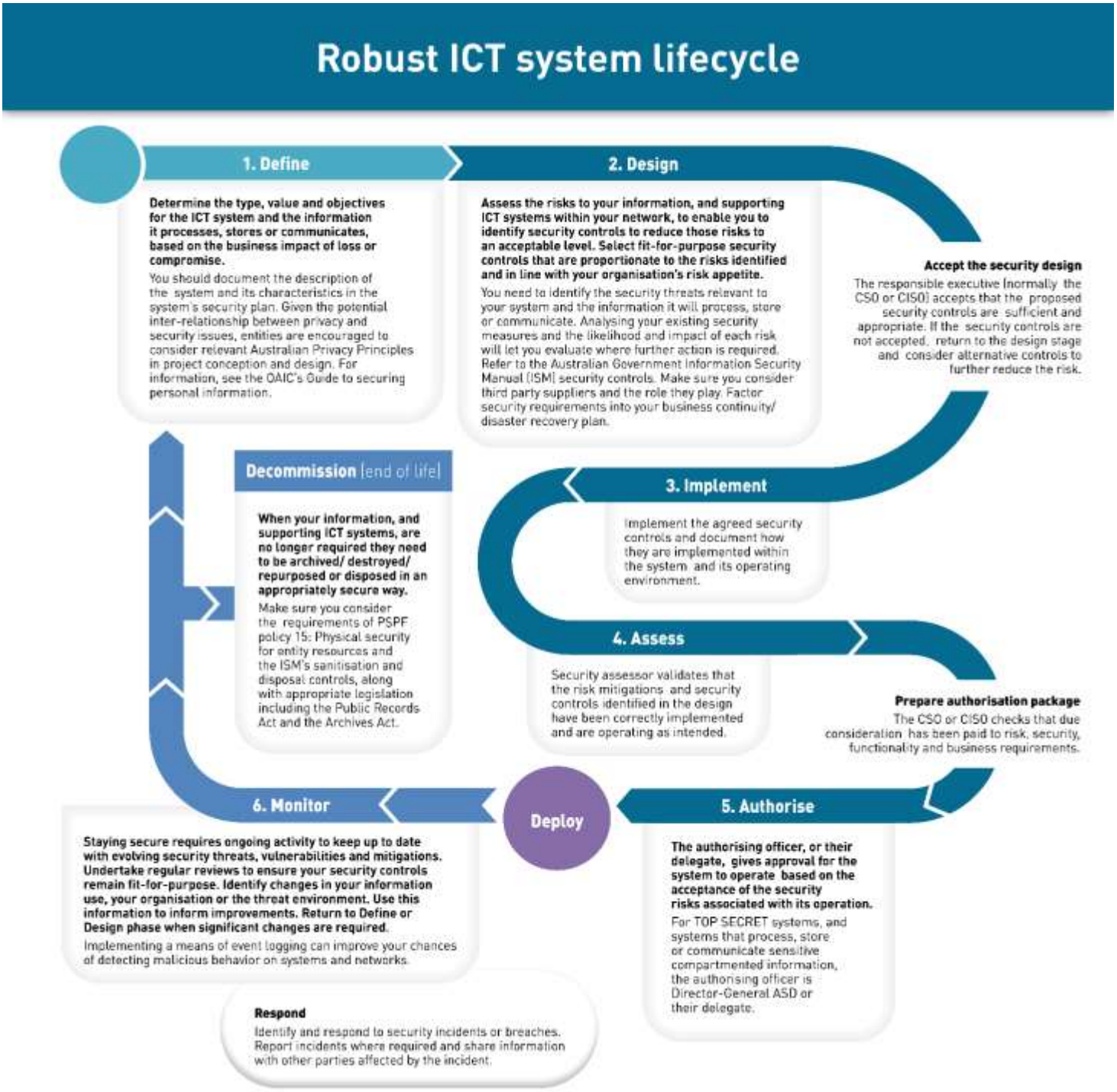
15. Authorisation to operate is not permanent. During the lifecycle of an ICT system, it may require reauthorisation to operate or eventually be decommissioned (ie disposal at the end of its life). Examples of events that may trigger reauthorisation for an ICT system include:
    a. changes in the security policies relating to the system
    b. detection of new or emerging cyber threats to the system or its operating environment
    c. discovery that implemented security controls are not as effective as planned
    d. major cyber security incident involving the system
    e. major architectural changes to the system or its user base.

### C.2.1 Six step risk-based approach to cyber security

16. **Requirement 1** mandates that decisions to authorise (or reauthorise) an ICT system to process, store or communication information be based on the ISM's risk-based approach to cyber security. This risk-based approach, recommended by the ACSC in the ISM, comprises the following six steps:
    a. **Step 1 – Define the ICT system**: determine the value of each ICT system and the information it processes, stores and communicates, based on an assessment of the business impact of loss or compromise.
    b. **Step 2 – Select security controls:** identify the security risks to each ICT system and select fit-for-purpose security controls that are proportionate to the security risks identified and consistent with the entity's agreed risk tolerances.
    c. **Step 3 – Implement security controls**: implement the selected security controls to reduce identified security risks to an acceptable level of residual risk and document how these security controls are implemented within the ICT system and its operating environment.
    d. **Step 4 – Assess security controls**: assess the security controls for each ICT system to validate they have been correctly implemented and are operating as intended.
    e. **Step 5 – Authorise the ICT system:** authorise ICT systems to operate based on the acceptance of the residual security risks associated with their operation. See **Table 1** for determining authorities.
    f. **Step 6 – Monitor the ICT system:** monitor the security posture of each ICT system to identify and respond to cyber threats and security risks while ensuring security controls remain effective and fit-for-purpose for the system's operating and threat environment. This includes incorporating processes to ensure the accuracy and integrity of data captured and held in the ICT system. If significant or extensive adjustments are identified, it is recommended to return to the 'define the ICT system' phase of the lifecycle to recommence authorisation for that ICT system to operate.

17. **Figure 1** outlines the ISM's risk-based process for authorising an ICT system to operate and managing security risks during all stages of the lifecycle of the system. It also notes the need to consider when to decommission (or dispose of) an ICT system at the end of its life. For guidance on disposal of an ICT system at the end of its life, see PSPF policy 15: Physical security for entity resources and the ISM's *Guidelines for ICT Equipment*.

**Figure 1 Robust ICT system lifecycle**




## C.2.2 Determining authority for authorisation of ICT systems to operate

18. **Requirement 1** requires that all ICT systems are authorised to operate by the relevant determining authority based on the acceptance of any residual security risks associated with the operation of the ICT system before authorisation to operate is granted.

19. **Table 1** outlines who the determining authority is for each type of ICT system, and who can perform the security assessor role.

20. **Security assessor:** reviews the system architecture, including security documentation, and assesses the implementation and effectiveness of security controls. These assessments are typically undertaken by an Information Security Registered Assessors Program (IRAP) assessor or entity personnel with the appropriate capability.

21. **Authorising officer:** reviews the authorisation package and makes an informed risk-based decision as to whether the security risks associated with an ICT system's operation are acceptable or not, and grants

approval for the system to operate. The authorisation package includes the ICT system's system security plan, incident response plan, continuous monitoring plan, security assessment report, and plan of action and milestones. The authorising officer is typically the accountable authority or Chief Security Officer. However, this function can be delegated to another suitably senior officer where required, for example the Chief Information Security Officer. For TOP SECRET systems and systems that process, store or communicate TOP SECRET or sensitive compartmented information, ASD is the authorising officer.

22. See the ISM for further information on conducting security assessments and the authorisation package.
23. It is recommended that entities document the name and position of the authorising officer for each ICT system, particularly where the accountable authority has delegated this responsibility to another officer.
24. To ensure accountability for security decisions relating to ICT systems, including decisions to accept residual security risks, it is further recommended that these decisions are captured in the system's security documentation.

**Table 1 Determining authority for authorisation of ICT systems**

| Type of ICT system | Security assessor | Determining authority (Authorising officer) |
|---|---|---|
| TOP SECRET systems | Australian Signals Directorate assessor (or their delegate) | Director-General Australian Signals Directorate (or their delegate) |
| TOP SECRET sensitive compartmented information systems | Australian Signals Directorate assessor (or their delegate) | Director-General Australian Signals Directorate (or their delegate) |
| SECRET systems | Entity assessor or Information Security Registered Assessors Program (IRAP) assessor | Accountable authority or Chief Security Officer (or their delegate) |
| PROTECTED and OFFICIAL systems (including OFFICIAL: Sensitive) | Entity assessor or IRAP assessor | Accountable authority or Chief Security Officer (or their delegate) |
| For multinational and multi-entity systems | Determined by agreement between the parties involved | Determined by a formal agreement between the parties involved |
| Outsourced information technology and cloud services (with the exception of TOP SECRET systems and secure internet gateways intended for use by multiple entities) | Entity assessor or IRAP assessor | Accountable authority or Chief Security Officer (or their delegate) |

### C.2.3 Outsourced information technology and cloud services

25. Obligations for protecting Australian Government information that is processed, stored or communicated via an outsourced information technology or cloud service provider are no different than using an internal entity service. The same authorisation to operate framework to manage security risks during the lifecycle of the ICT system/service still applies.
26. As outlined in PSPF policy 9: Access to information, when considering the suitability of a particular outsourced information technology or cloud service provider and their services, entities are required to ensure that those who access sensitive or classified information have an appropriate Australian Government security clearance, briefings and a need-to-know. For example, if the service provider's personnel hold an Australian Government security clearance commensurate with the information being stored, processed and transmitted in their cloud services, this presents the lowest risk to sensitive or classified information being exposed to uncleared personnel or foreign nationals.
27. In accordance with the Australian Government Secure Cloud Strategy, entities are able to self-assess cloud service providers and cloud services using the risk-based approach to cyber security outlined in the ISM. Entities are strongly recommended to use the ACSC's guidance on cloud security when performing a security assessment to determine the suitability of a particular cloud service provider and its cloud services. See *Anatomy of a Cloud Assessment and Authorisation*.

28. The PSPF general obligation for information security applies even when information is processed, stored or communicated via outsourced information technology or cloud services.[2] Entities remain responsible for the security risks associated with any procurement, including cloud services procured through a cloud services provider. For further information on requirements relating to service providers, see PSPF policy 6: Security governance for contracted service providers.

29. For further ACSC guidance on outsourcing of information technology and making decision about cloud service providers see the ISM's *Guidelines for Outsourcing*.

#### C.2.3.1 Foreign-owned service providers or cloud services

30. Entities who are considering the use of foreign owned information technology or cloud service providers should also take into account the following guidance in their considerations for authorisation of ICT systems.

    a. PSPF policy 6: Security governance for contracted service providers outlines requirements for managing security risks associated with any procurement, including the potential security risks associated with foreign involvement. See also the ISM's *Guidelines for Outsourcing* for foreign owned service providers and offshore services and *Anatomy of a Cloud Assessment and Authorisation*.

    b. PSPF policy 7: Security governance for international sharing outlines requirements for providing foreign contractor access to sensitive or classified information. This includes any foreign individual or legal entity entering into, or bound by, a classified contract and includes subcontractors.

    c. PSPF policy 9: Access to information outlines the Australian Government security clearance, briefings and a need-to-know requirements for access to sensitive or classified information.

    d. ASIO T4 Protective Security Circular 149 – *Physical security certification of outsourced ICT facilities* (available to Government personnel on GovTEAMS) provides additional guidance on PSPF implementation in the outsourced ICT facility/data centre environment, including considering the security risks of using foreign-owned providers and storing data offshore.

#### C.2.3.2 Data centres

31. The need to establish security terms and conditions in contracts, outlined in PSPF policy 6: Security governance for contracted service providers, also apply to data centres.

32. The Digital Transformation Agency's (DTA) Whole-of-government Hosting Strategy provides policy guidance on securely hosting government data in facilities such as data centres and associated infrastructure. The DTA also manages the Data Centre Facilities Supplies Panel. Non-corporate Commonwealth entities are required to use this panel when buying data centre space and services. Entities remain responsible for assessing any foreign involvement risk in any procurement under this panel.

33. ASIO T4 Security managers guide – *Data centre security* (available to Government personnel on GovTEAMS) provides guidance on assessing the security risks of contracting outsourced data centre providers.

34. For ACSC guidance on data centres, see ISM's *Guidelines for Outsourcing*.

## C.3 Secure internet gateways

35. A gateway is an information flow control mechanism–it manages information flows between connected networks from different security domains.

36. Secure internet gateways (SIGs) play a vital role in securing ICT systems and are one element of a layered defensive strategy. By adopting a set of common services, government benefits from a baseline level of protection at the network perimeter. A number of high-risk threats to ICT systems (for example, distributed denial of service attacks, botnets, malware, web application attacks and web-based attacks) are amenable to efficient mitigation through appropriately configured SIGs. At the same time, entities require the

[2] Under s95B of the Privacy Act, entities are required to take contractual measures to ensure that a contracted service provider (including an information technology or cloud service provider), does not do an act, or engage in a practice, that would breach an APP. For guidance, see the PSPF policy 6: Security governance for contracted goods and service providers.

flexibility to source additional security services in a manner that best suits their operational needs and risk environment.

37. **Requirement 2** mandates that entities must protect their internet-connected ICT systems, and the information they process, store or communicate, by implementing a SIG that meets ASD requirements.

38. For general guidance on gateways, see the ISM's *Guidelines for Gateways*. Alternatively, for connections between security domains involving SECRET or above ICT systems, see guidance on Cross Domain Solutions in the ISM's *Guidelines for Gateways*.

39. The ACSC continuously assesses cyber threats and security risks and periodically issues updated guidelines via the ISM, as well as indicators of compromise for use with intrusion detection systems within gateway environments. For any questions on ACSC guidance, contact the ACSC via https://www.cyber.gov.au/acsc/contact or call 1300 CYBER1 (1300 292 371).

### C.3.1 Determining authorities for secure internet gateways, either government or commercial

40. **Table 2** outlines who can perform the security assessor role, and the Certification Authority and Accreditation Authority determining authority roles for secure internet gateways. It is recommended that entities document the name and position of the Certification Authority and Accreditation Authority for each service, particularly where the accountable authority has delegated the Accreditation Authority responsibility to another officer.

41. **Security assessment**: reviews the SIG architecture, including security documentation, and assesses the implementation and effectiveness of security controls.

42. **Certification**: is awarded when the Certification Authority is satisfied that the security controls for the SIG have been implemented and are operating effectively.

43. **Accreditation**: is awarded when the Accreditation Authority accepts the residual security risks to the SIG and grants approval for the SIG to operate.

**Table 2 Determining authorities for secure internet gateways, either government or commercial**

| Intended use | Determining authorities | | |
|---|---|---|---|
| | Security assessor | Certification Authority | Accreditation Authority |
| Commercial or government secure internet gateway (intended for use by multiple entities across government) | Joint Australian Signals Directorate (ASD) assessor and IRAP assessor | Head Australian Cyber Security Centre (or their delegate) | Accountable authority or Chief Security Officer (or their delegate) |
| Commercial or government secure internet gateway (intended for use by a single entity) | Entity assessor or IRAP assessor | Chief Security Officer (or delegated security advisor) | Accountable authority or Chief Security Officer (or their delegate) |

# D. Find out more

44. Other policies and information include:

    a. Australian Signals Directorate advice:

        i. Australian Government Information Security Manual

        ii. Information Security Registered Assessors Program (IRAP)

        iii. ASD Certified Gateway Services

        iv. Anatomy of a Cloud Assessment and Authorisation

        v. Cloud Computing Security Considerations

        vi. Cloud Computing Security for Cloud Service Providers

        vii. Cloud Computing Security for Tenants

viii. Cyber Supply Chain Risk Management

b. Office of the Australian Information Commissioner.

## D.1 Change log

**Table 3 Amendments in this policy**

| Version | Date | Section | Amendment |
|---|---|---|---|
| v2018.1 | Sept 2018 | Throughout | Not applicable. This is the first issue of this policy |
| v2018.2 | March 2020 | Table 2 and C.2.1 | Changes to reflect outcomes of the Review of Cloud Services Certification Program. Requested by ASD. |
| v2018.3 | July 2020 | Whole document | Following a review to realign policy 11 with the ISM, this version contains new core and supporting requirements and related guidance. Developed in consultation with ACSC and DTA. Approved by the Government Security Committee on 18 August 2020. |