Australian Government
Attorney-General's Department

Protective Security Policy Framework

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. Secure ICT systems protect the integrity (and facilitate the availability) of the information that entities process, store and communicates.

B. Requirements

B.1 Core requirement

> ***Each entity must have in place security measures during all stages of ICT systems development. This includes certifying and accrediting ICT systems in accordance with the Information Security Manual when implemented into the operational environment.***

B.2 Supporting requirements

Supporting requirements for robust ICT systems

#	Supporting requirements
Requirement 1. ICT systems	When establishing new ICT systems, or implementing improvements to current ICT systems (including software development), entities **must** address security in the early phases of the system's development life cycle. This includes during the system concept development and planning phases, and then in the requirements analysis and design phases.
Requirement 2. Certification and accreditation	Entities **must not** process, store or communicate sensitive or classified information on an entity ICT system, unless the residual security risks to the system and information have been recognised and accepted in accordance with the Information Security Manual.
Requirement 3. System monitoring	Entities **must** ensure their ICT systems (including software) incorporate processes for audit trails and activity logging in applications, to ensure the accuracy and integrity of data captured or held.
Requirement 4. Secure internet gateways	Entities **must** obtain their internet connection services for their ICT systems through a secure gateway meeting Australian Signals Directorate requirements for managing security risks.

C. Guidance

C.1 Security measures during ICT system development or improvement

2. When establishing new ICT systems or implementing improvements to current ICT systems, it is more cost effective to address security issues during conception, architecture and design, than retrofitting security protections at a later time.[1]

3. As such, **Requirement 1** mandates that entities must address security in the early phases of ICT system development. **Table 1** outlines key security issues that may warrant consideration during system development; ongoing consideration of these security matters throughout the ICT system's life cycle is important to maintaining information 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 Guide to securing personal information.

4. For guidance, see the Australian Signals Directorate (ASD) Information Security Manual (ISM).

Table 1 Security issues to consider for new ICT systems or when implementing improvements to current systems

Security issue	Matters for consideration
Information security documentation	Preparing relevant documentation supports implementing PSPF policy and ISM guidance. Preparing a security risk management plan is mandated in the PSPF policy: Security planning and risk management.
Information security monitoring	Vulnerability management includes monitoring and managing vulnerabilities in, and changes to, a system that can provide valuable information about exposure to threats. Change management includes implementing routine and urgent changes to software or systems to maintain security (including if the change triggers the need for reaccreditation).
Communications security	Infrastructure security includes goods cable management and emanations security regimes that help entities maintain the integrity and availability of communications infrastructure as well as the confidentially of information: a. Cable management practices can protect information from deliberate or inadvertent access. b. Countermeasures reduce the risk of information being intercepted and systems compromised. Systems and devices security includes measures that minimise data spills or unauthorised disclosure of information as data flows in and out of digital gateways.
Product security	Entities need assurance that products with a security function perform as claimed by the vendor and provide the necessary security to mitigate security threats. Assurance is achieved through formal and impartial evaluation. ASD manages a number of evaluation programs and the results are listed on an Evaluated Products List. For other products, vendor support can be a prime method of ensuring product security.
Media security	Implementing sound security practices when connecting, storing, transferring, sanitising, destroying or disposing of media plays a major role in preventing classified or sensitive data spills and avoiding malicious attacks. Media security is particularly important when decommissioning an ICT system. The PSPF policy: Sensitive and classified information, supported by the ISM, provides guidance on the sanitisation or destruction of ICT media and equipment.
Software security	It is important to implement and maintain measures to protect against software vulnerabilities that may be used to undermine the integrity or availability of systems or information.
Access control	Well-structured and robust ICT systems allow necessary access for personnel to undertake their work while protecting information, technology and intellectual property. The PSPF policy: Access to information requires entities to control access to ICT systems, networks (including remote access), infrastructure and applications. See the PSPF policy: Access to information supporting requirement 5 (and related guidance).
Administrator rights	Restricting administrative privileges is one of the most effective ways to safeguard ICT systems. For policy and guidance on restrictions of administrative privileges, see the PSPF policy: Safeguarding information from cyber threats **Requirement 3** (and related guidance).
Network security	Network management practices and procedures assist in identifying and addressing network structure or configuration vulnerabilities.
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.
Cross domain security	Mitigating risks by securely managing data flows between different security domains includes: a. deploying and configuring gateways to manage information flow paths (ingress and egress of traffic) across approved systems on entity networks b. implementing gateway firewalls to protect against intrusions, particularly for sensitive networks (AUSTEO or AGAO) c. using diodes to protect against data spills and malicious actors seeking to use information flow paths to intrude or attack information d. allowing web access while protecting against the execution and spread of malicious software e. sharing peripherals between ICT components and ensuring unauthorised information does not pass between security domains.
Data transfers and content filtering	Implement procedures to ensure that content leaves a security domain in a secure manner. Apply content filtering techniques to reduce the risk of unauthorised or malicious content crossing a security boundary.

C.2 ICT accreditation framework

5. The PSPF requires entities to certify that an appropriate level of security is being applied to their ICT systems and that residual risks have been accepted by a relevant accreditation authority. This will provide the confidence that ICT products meet security needs, address known vulnerabilities and remain secure. An impartial (and in some cases, independent) evaluation or security assessment can be a valuable tool in informing certification and accreditation decisions.

6. Key elements of an indicative accreditation framework are:

   a. **Security assessment or audit** that reviews the system architecture, including information security documentation and assesses the implementation and effectiveness of security measures. These assessments are typically undertaken by an information security registered assessor (IRAP). For information about conducting security assessments, refer to the ISM.

   b. **Certification** is awarded when an entity is satisfied that security measures have been implemented and are operating effectively to ensure the system's integrity and confidentiality. Certification is typically granted by an entity Chief Security Officer or delegated security advisor. However, ASD is the certification authority of systems that process, store or communicate TOP SECRET information. For guidance, refer to the ISM.

   c. **Accreditation** is awarded when an entity accepts the residual security risk to a system (and the information it processes, stores or communicates) and grants approval for the system to operate. Accreditation is typically granted by the accountable authority (or at least the CSO unless otherwise stated in **Table 2**, or the certification authority). However, ASD is the accreditation authority of systems that process, store or communicate TOP SECRET information. For guidance, refer to the ISM.

7. Accreditation is not permanent. Recertification and reaccreditation may be triggered by:

   a. expiry of the accreditation due to the passage of time

   b. changes in the business impact associated with the system (eg the integrity of a system is reassessed or the classification raised)

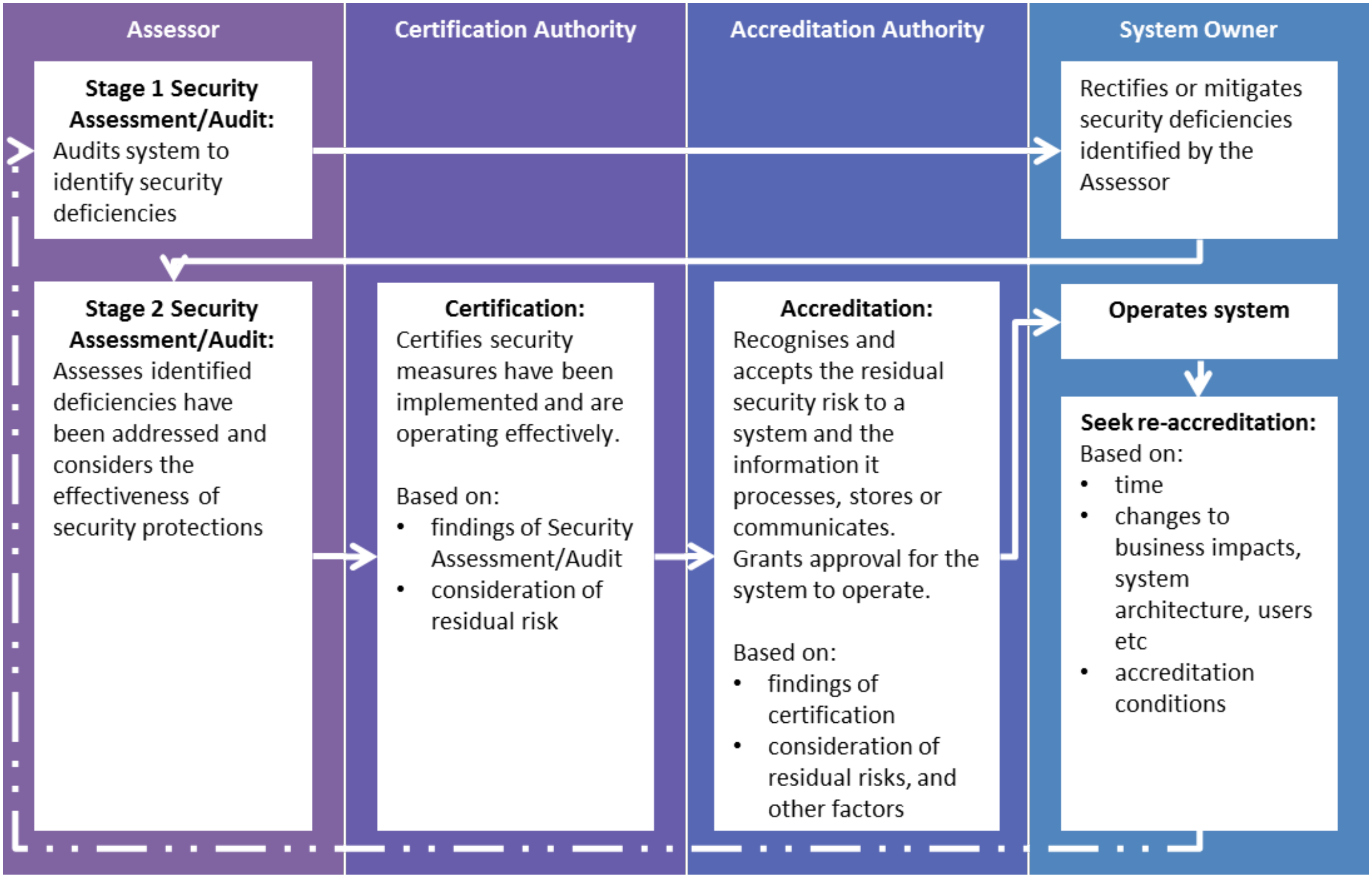
   c. significant changes to the architecture of the system or the security controls that it implements

   d. changes to users of the system, particularly in regard to foreign nationals and privileged users

   e. any other conditions stipulated.

8. **Figure 1** outlines an indicative process for awarding ICT system certification and accreditation. **Table 2** identifies who can make decisions relating to certification and accreditation for different types of ICT systems.

Figure 1 Indicative process for system certification and accreditation



Stage 1 Security Assessment/Audit: Audits system to identify security deficiencies

Rectifies or mitigates security deficiencies identified by the Assessor

Stage 2 Security Assessment/Audit: Assesses identified deficiencies have been addressed and considers the effectiveness of security protections

Certification: Certifies security measures have been implemented and are operating effectively.

Based on:

- findings of Security Assessment/Audit
- consideration of residual risk

Accreditation: Recognises and accepts the residual security risk to a system and the information it processes, stores or communicates. Grants approval for the system to operate.

Based on:

- findings of certification
- consideration of residual risks, and other factors

Operates system

Seek re-accreditation: Based on:

- time
- changes to business impacts, system architecture, users etc
- accreditation conditions

Table 2 Determining authorities

ICT system type	Determining authority		
	Security assessment (assessor)	**Certification authority**	**Accreditation authority**
TOP SECRET systems	ASD or IRAP assessor	ASD	Director-General ASD (or delegate)
SECRET systems	Entity security advisor (or IRAP assessor, or other security professional)	Entity Chief Security Officer (or delegated security advisor)	Accountable authority (or delegated to the Chief Security Officer)
PROTECTED and OFFICIAL systems	Entity security advisor (or IRAP assessor, or other security professional)	Entity Chief Security Officer (or delegated security advisor)	Entity Chief Security Officer (or delegate) Note i
For systems that process, store or communicate caveated or compartmented information	Entity security advisor (or IRAP assessor, or other security professional)	Accountable authority (or delegated to Chief Security Officer). Note, there may be a mandated certification authority external to the entity operating the system	Director-General ASD (or delegate)
For multinational and multi-entity systems	Determined by agreement between the parties involved	Determined by a formal agreement between the parties involved	Determined by a formal agreement between the parties involved
For commercial providers providing ICT services	Security advisor (or IRAP assessor, or other security professional) of the entity sponsoring the provider	Chief Security Officer (or delegated security advisor) of the entity sponsoring the provider	Head of the supported organisation or their authorised delegate, which is strongly recommended to be the Chief Security Officer

ICT system type	Determining authority		
	Security assessment (assessor)	**Certification authority**	**Accreditation authority**
For providers of gateway or cloud services, either government or commercial:			
a. intended for use by multiple entities across government	Entity security advisor (or IRAP assessor, or other security professional)	ASD can perform the role of the certification authority as an independent third party	Accountable authority (or delegated to Chief Security Officer) [Note ii]
b. private cloud, or intended for use by a single entity	Entity security advisor (or IRAP assessor, or other security professional)	Entity Chief Security Officer (or delegated security advisor)	Accountable authority (or delegated to Chief Security Officer) [Note ii]

Table 2 notes:

[i] The entity Chief Security Officer (or delegate) represents the minimum level for an accreditation authority for PROTECTED and OFFICIAL systems. An entity may wish elevate accreditation decisions to the accountable authority to align with accreditation of SECRET systems and to ensure whole of enterprise risks are considered.

[ii] For TOP SECRET systems, accreditation is determined by ASD.

C.2.1 Cloud services

9. The PSPF general obligation for ICT security applies even when information is processed, stored or communicated via cloud services.[2]

10. Given public and community cloud services can be procured and consumed by many (not just a single entity), efficiencies can be gained from ASD assessing and certifying cloud services (to be shared with all entities, not just a single entity). A list of ASD-certified providers is available on the ASD website at ASD Certified Cloud Services List.

11. Entities can choose to certify cloud services independent of an ASD certification, particularly for private cloud services where the service has only one customer, or where a cloud service is not widely used. As for other systems, accreditation of a cloud service is the responsibility of the entity with the exception for TOP SECRET systems where accreditation is determined by ASD.

C.3 ICT system monitoring

12. Monitoring ICT systems through event logging improves the chances that malicious behaviour will be detected. Conducting regular audits of event logs will help detect, attribute and respond to any security issues. **Requirement 3** mandates that entities ensure their ICT systems (including software) incorporate processes for audit trails and activity logging, to ensure the accuracy and integrity of data captured or held.

13. **Table 3** identifies recommended events to log for ICT systems. Further guidance on events to log for databases, operating systems and web applications is available in the ISM.

Table 3 Recommended audit logging events for ICT systems

Recommended audit logging events
Successful and failed elevation of privileges
Security related system alerts and failures
User and group additions, deletions and modification to permissions
Unauthorised access attempts to critical systems and files

14. To assist with the correlation of logged events, it is important to establish an accurate time source, and use it consistently across systems.

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

C.4 Secure internet gateways

15. 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 SIG services, government benefits from a baseline level of protection at the network perimeter. A number of high-risk threats to ICT systems (eg distributed denial of service, botnets, malware, web application attacks, web-based attacks) are amenable to efficient mitigation through appropriately configured SIGs. At the same time, entities require the flexibility to source additional security services in a manner that best suits their operational needs and risk environment.

16. ASD periodically assesses national cyber risk and issues technical guidelines on SIG to deliver mitigation outcomes. This includes advice for coordinated internet monitoring and intrusion detection capability. **Requirement 4** mandates that entities obtain their SIG services from providers meeting ASD requirements.

D. Find out more

17. Other policies and information include:

    a. Australian Signals Directorate advice:

        i. Information Security Manual

        ii. Information Security Registered Assessors Program (IRAP)

        iii. Cloud Computing Security Considerations

    b. Office of the Australian Information Commissioner.

D.1 Change log

Table 4 Amendments in this policy

Version	Date	Section	Amendment
v2018.1	Sep 2018	Throughout	Not applicable. This is the first issue of this policy