Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Executive guidance

Gateway Security Guidance Package

First published: July 2022

Last updated: July 2025

Introduction

This executive guidance is for senior or executive decision-makers who are accountable for the design, procurement, operation, maintenance and disposal of gateway solutions.

Gateways provide organisations with cyber security protection at the network perimeter. A gateway is a boundary system that separates different security domains. It allows an organisation to enforce security policies for data transfers between different security domains.

Gateways are an important component of a layered defence-in-depth cyber security approach. They can be shared between multiple organisations, providing the benefits of a shared suite of defences. A common use case for gateway deployment is between an organisation's internal network and the internet.

Since the release in July 2022 of the Australian Signals Directorate's Australian Cyber Security Centre's (ASD's ACSC) *Gateway Security Guidance Package* (the Gateway Guidance), there have been significant advances in technology and changes to service delivery. Advancements and updates to gateway requirements under the Department of Home Affairs *Protective Security Policy Framework* (PSPF) Release 2025, including the new *Australian Government Gateway Security Standard* (the Gateway Standard) have prompted updates to the Gateway Guidance, building on the approach adopted in the initial 2022 release.

Under the Gateway Standard, non-corporate Commonwealth entities (NCEs)[1] are encouraged to adopt a risk-based authorisation model. This approach is consistent with the Information Security Manual (ISM), the intent of the Foundations for modern defensible architecture, and by leveraging cloud security offerings, such as Security Service Edge (SSE) solutions.

[1] Non-corporate and corporate Commonwealth entities are government bodies that are subject to *the Public Governance, Performance and Accountability Act 2013*. More information: Non-corporate Commonwealth entity (NCE) | Department of Finance

Purpose of the gateway security guidance package

The Gateway Guidance is not a policy, certification framework or checklist. Organisations should consider their own unique operating environment and requirements alongside the Gateway Guidance.

The Gateway Guidance recognises the diverse nature of current enterprise information and communications technology (ICT) environments, which include on-premises, cloud and mobile technologies. It does not recommend specific technologies, but allows organisations to interpret and apply the guidance to align with their cyber security needs. Organisations should consider this guidance alongside their relevant policies, frameworks and needs.

Definition of a gateway

The definition of a gateway in the Information security manual (ISM) is, 'Gateways securely manage data flows between connected networks from different security domains'.

Gateways are a set of capabilities that enable an organisation to securely:

- provide services to external parties
- exchange information with others
- support remote work
- operate across trusted and untrusted networks (including the internet).

A gateway is a network boundary solution responsible for controlling the flow of data into and out of an organisation's ICT environment or security domain. This position in the network means that gateways are critical implementation points. They provide a broad range of security capabilities that enforce an organisation's security policies before allowing access into or out of the organisation's network.

A gateway should:

- apply risk mitigations and cyber security controls to the flow of data between security domains
- provide visibility of transiting data according to an organisation's policies.

All stakeholders involved in the design, procurement, operation, maintenance and disposal of an organisation's gateways need to understand the design principles and objectives of gateway controls.

Organisations can use gateway solutions through various delivery models, including on-premises, cloud-native, hybrid or managed service provider models. With cloud-native or managed service provider models, an organisation may use a gateway as an abstracted set of security services and capabilities rather than as specific equipment or functionality.

Cross Domain Solutions

Organisations can use a Cross Domain Solution (CDS) as part of an internet gateway. A CDS is a system capable of implementing comprehensive data flow security policies with a high level of trust between two or more different security domains. CDSs are implemented between SECRET or TOP SECRET networks and any other networks belonging to different security domains. They can also be used for networks that operate at or below PROTECTED level that connect to the internet, where high-assurance security policy enforcement capability is needed to manage risk.

Refer to the ISM and resources for Cross Domain Solutions when gateway solutions contain at least one security domain classified SECRET or TOP SECRET, or classified at PROTECTED or below where a high-assurance solution is required to manage identified threats and resulting harm.

The threat environment

ASD's ACSC has observed malicious actors targeting 'edge devices'. These devices are typically deployed in gateways - as routers, firewalls and VPN concentrators - and act as security intermediaries between internal networks and the internet. Edge devices are attractive targets as they often hold sensitive information, can be accessed from external networks, and act as enforcement points for organisational security policies. If compromised, these devices give attackers a foothold to bypass perimeter defences, intercept sensitive traffic (including classified information), or gain access to internal systems.

The rapid exploitation of newly disclosed vulnerabilities is now common tradecraft for malicious actors. Both skilled and unskilled malicious actors continually conduct scanning and reconnaissance against internet-accessible networks to identify unpatched devices that can be exploited.[2] Methods used to target Australian networks are constantly expanding and evolving. This highlights the need to continually improve an organisation's security posture to help mitigate the risks.

Senior and executive decision-makers are responsible for managing risks and maintaining the confidentiality, integrity and availability of their organisation's data and systems. An organisation can mitigate cyber security risks and threats by implementing a broad range of controls across its ICT environment, including gateways.

For executive and technical guidance on edge devices, refer to securing edge devices.

For more information on the current threat environment, refer to ASD's ACSC reports and statistics, which includes the *Annual Cyber Threat Report* and the *Commonwealth Cyber Security Posture Report*.

[2] An 'unpatched' device is any device (including software running on a device) that has not been kept up to date with the latest security updates, as recommended and provided by the relevant vendor.

Requirements for government organisations

Australian Government organisations, particularly NCEs, must operate within several policies and frameworks. These frameworks govern how NCEs design, procure, operate, maintain and dispose of gateway solutions.

Senior and executive decision-makers are accountable for ensuring their organisation complies with these requirements. At a minimum, they should be familiar with the frameworks described in this guidance. While these requirements generally do not apply to private sector organisations, service providers and vendors offering products or services to government organisations should also be aware of them.

NCEs implementing gateways that need to operate at the SECRET or TOP SECRET security levels should follow this guide along with guidance on Cross Domain Solutions. For these high-security environments, CDS requires extra services and additional monitoring and logging due to the serious risk of leaking highly classified information. NCEs that design, procure, operate, maintain and dispose of CDS services in these environments should contact ASD's ACSC for specific advice.

Protective Security Policy Framework

NCEs must apply and adhere to the PSPF when designing, procuring, operating, maintaining and disposing of gateways. This includes when using the gateway services of another organisation or service provider. NCEs cannot transfer this accountability to a third-party gateway service provider or other NCEs.

Section 13.3 of the PSPF requires that NCEs must only process, store or communicate information and data on ICT systems where an Authorising Officer (or their delegate) with appropriate authority has authorised the system to operate based on the acceptance of the residual cyber security risks associated with its operation. The relevant Accountable Officer for a system, including gateways, must understand the risks associated with using the system and should review the system's security plan regularly. As per the PSPF, the decision to authorise (or re-authorise) an ICT system to operate, including gateways, must be based on the ISM's six-step, risk-based approach for cyber security (**Figure 1**).

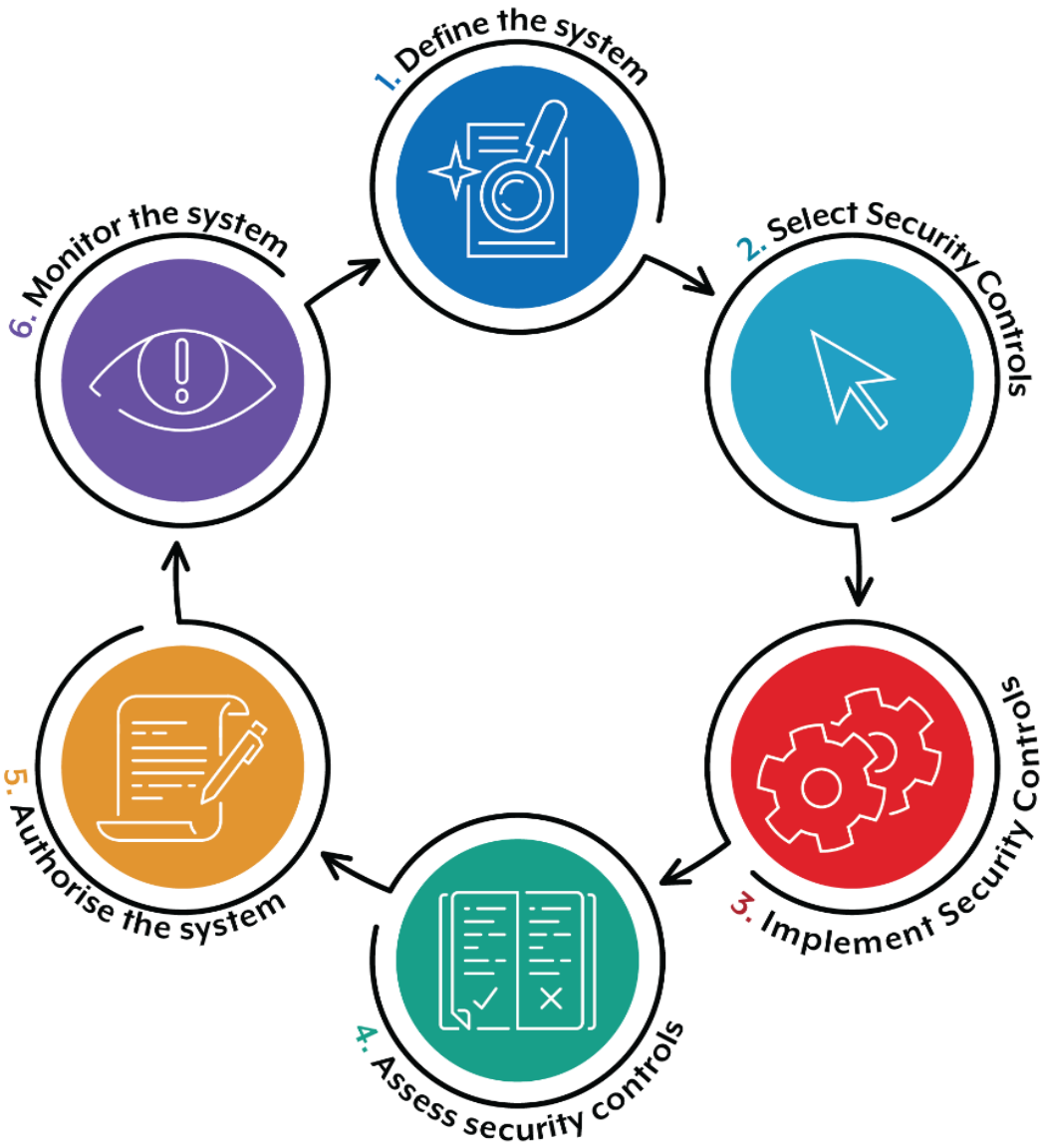

Figure 1: ISM's six step risk-based approach for cyber security

Gateway Security Standard

The Gateway Standard replaces the *Australian Government Gateway Policy* (Gateway Policy). The Gateway Standard describes the strategic direction for Australian Government use of gateway services and sets the minimum security standard expected from Commonwealth entities when using gateway capabilities, including SSE. The Gateway Standard is a part of a broader coordinated uplift of the Australian Government's cyber security consultation agenda led by the Department of Home Affairs (Home Affairs).

Shield 4 of the *2023-2030 Australian Cyber Security Strategy* highlights the importance of this uplift. To support this critical agenda, Home Affairs is consolidating a number of government IT infrastructure policies under a cohesive Resilient Digital Infrastructure strategy. This includes reviewing and updating the Gateway Policy (now the Gateway Standard) and the Secure Cloud Strategy, and integrating reforms to the *Hosting Certification Framework*.

Infosec Registered Assessors Program

Under the Infosec Registered Assessors Program (IRAP), ASD's ACSC endorses individuals from the private and public sectors to provide security assessment services. IRAP aims to enhance the security of broader industry and Australian Government systems and data. Organisations should refer to the IRAP Consumer Guide for more information on how best to:

- engage an IRAP assessor
- prepare for an IRAP assessment
- understand the assessment process
- use the information provided in an IRAP assessment report.

For more information on the ISM controls relating to assessing gateways, refer to Guidelines for gateways.

Figure 2 shows best practice for organisations on how to assess and authorise gateways.

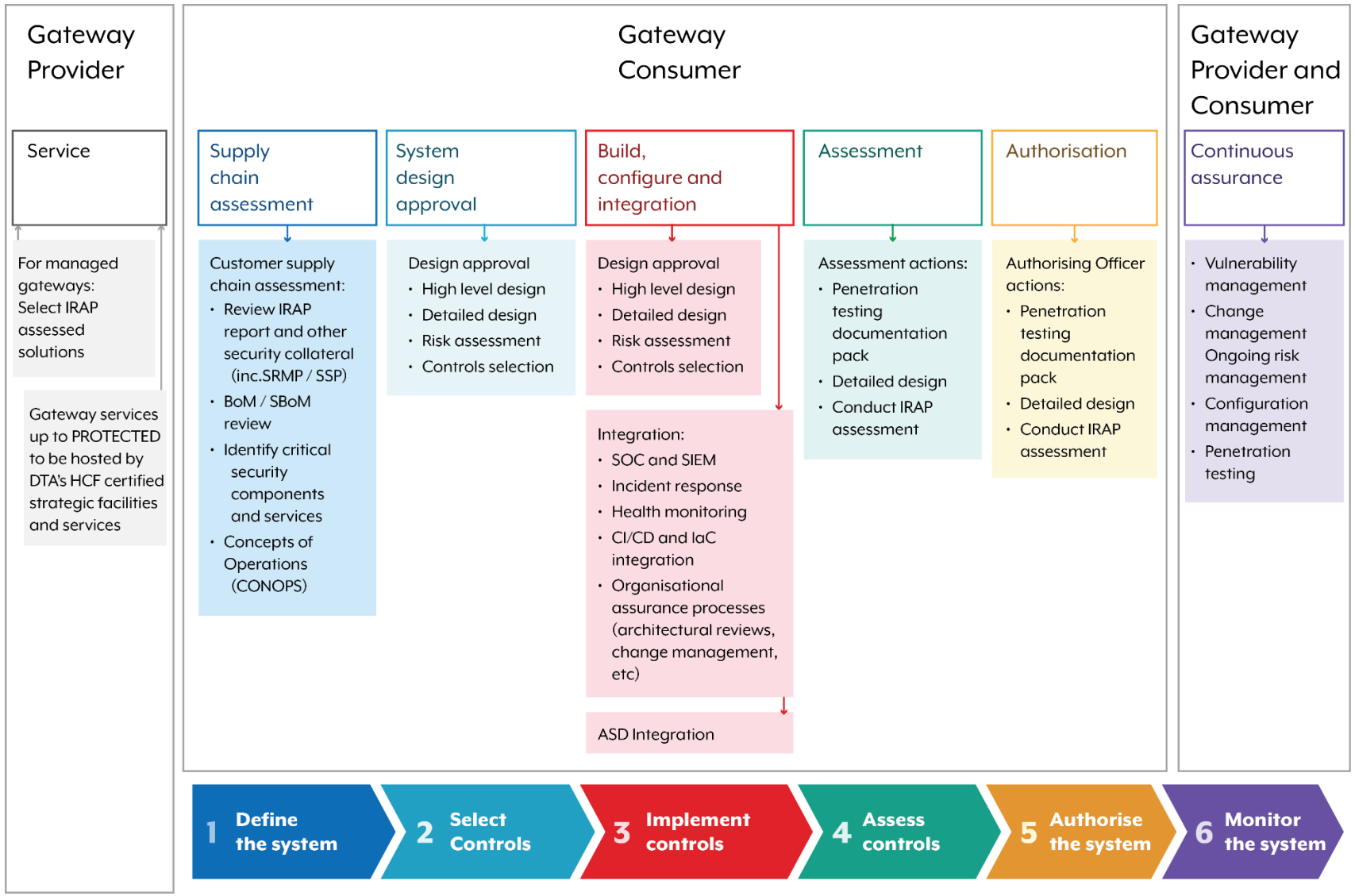

Figure 2: Assessing and authorising gateways

More information

For more information on topics covered in this guidance, refer to the following ASD's ACSC publications:

- Information Security Manual
- Strategies to mitigate cyber security incidents and the Essential Eight
- Security considerations for edge devices
- Fundamentals of Cross Domain Solutions
- Guidelines for gateways
- Implementing network segmentation and segregation
- Cyber security incident response planning: Executive guidance
- Cyber security incident response planning: Practitioner guidance

Contact us

Following substantial updates to the Gateway Guidance in July 2025, ASD's ACSC welcomes feedback to ensure it remains clear, relevant and useful. If you have any questions or feedback, you can write to us or call us on 1300 CYBER1 (1300 292 371).

The Gateway Guidance is being released in parallel with the Department of Home Affairs *Australian Government Gateway Security Standard*. We encourage interested stakeholders to provide feedback on the Gateway Standard directly to the Department of Home Affairs.

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre