Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Gateway security guidance package: Overview

First published: July 2022

Intent of the guidance

The *Gateway security guidance package* is designed to assist organisations to make informed risk-based decisions when designing, procuring, operating, maintaining or disposing of gateway services and captures contemporary better practices.

As gateway security functions are becoming readily available in cloud service offerings, gateway architectures are evolving. Hybrid and cloud-native gateways, combined with new ways of working, means that gateway architectures will look different in the future. This guidance package outlines how organisations should approach cybersecurity challenges to make their gateways more secure, flexible and adaptive to different architectures and delivery models.

The Australian Signals Directorate (ASD) has co-designed this guidance with key industry and government stakeholders through a consultative process.

Why is this guidance needed?

The changes to the Australian Government's gateway policy aims to create a risk-based authorisation model. The gateway policy update includes changes to the *Protective Security Policy Framework* (PSPF) that aligns the process for gateways with the existing Authorisation to Operate (ATO) process replacing the previous Certification Authority role performed by ASD. This empowers non-corporate Commonwealth entities (NCEs) to adopt a risk-based approach to gateways, and the flexibility to adopt the gateway solutions which best suit their security requirements.

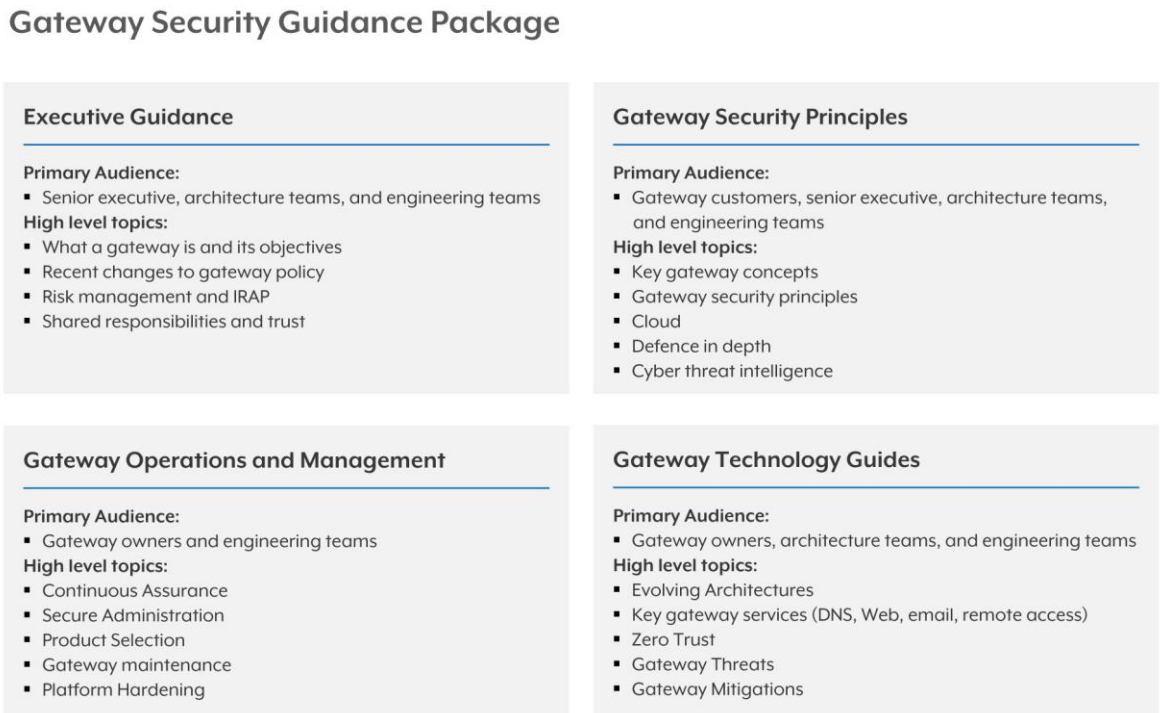
NCEs should gain assurance and inform themselves of the risks relating to designing, procuring, operating, maintaining and disposing of gateways through this guidance as well as the Infosec Registered Assessor Program (IRAP). As of 29 July 2022, ASD's *Certified gateways list* has been replaced by this guidance.

Intended audience

This guidance is one part of a package that forms the *Gateway security guidance package* written for audiences responsible for the design, procurement, operation, maintenance and disposal of gateways. When designing, procuring, operating, maintaining or disposing of a gateway, it is important to consider all the documents from the *Gateway security guidance package* at different stages of governance, design and implementation.

- The *Gateway security guidance package: Overview* document is intended to explain the structure of the *Gateway security guidance package* and is suitable for all audiences.
- The *Gateway security guidance package: Executive guidance* document is intended for decision-makers at an organisation's executive level.

- The *Gateway security guidance package: Gateway security principles* document is intended for senior executives, architecture teams and engineering teams.
- The *Gateway security guidance package: Gateway operations and management* document is intended for gateway operators.
- The *Gateway security guidance package: Gateway technology guides* document is intended for architecture teams, engineering teams and gateway operators.



While this guidance is primarily intended for Australian Government gateway consumers and their service providers, it can be used by any organisation designing, procuring, operating, maintaining or disposing of a gateway. In this *Gateway security guidance package*, the terms organisation, consumer and provider are used throughout the guidance for general use. Australian Government non-corporate Commonwealth entity is only used where there may be explicit requirements under the PSPF or other policy.

Policy and other considerations

The *Gateway security guidance package* should not be considered government policy or a checklist. ASD recommends organisations assess their gateways against their obligations under the PSPF, specifically as they relate to risk management (ISO 31000), ICT risk management (ISO 27001), the *Public Governance, Performance and Accountability Act 2013*, the *Commonwealth Procurement Rules*, and the guidance within the *Information security manual* (ISM) and the Department of Home Affair's, *Protective Security Policy Framework*.

NCEs should use the results of gateway IRAP assessments to inform their authorisation to operate decisions.

Commonwealth entities seeking to procure gateway services must consider the Department of Home Affairs' *Hosting Certification Framework* and ensure all sensitive and classified government data and associated infrastructure is hosted by a certified provider. The framework provides a process for government customers to attest to the risks of using a service.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).

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.

For more information, or to report a cybersecurity incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government

Australian Signals Directorate