Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre

Gateway security guidance package: Executive guidance

First published: July 2022

Executive summary

The Australian Signals Directorate (ASD) has designed a new approach to gateway services for non-corporate Commonwealth entities (NCEs). This reflects the significant advances in technology and the evolving needs of NCEs since the implementation of the Gateway Reduction Program in 2010. To support the new approach, this guidance has been published to inform all Commonwealth entities to which the *Protective Security Policy Framework* (PSPF) applies.

Gateways provide organisations with cybersecurity protection at the network perimeter. A gateway is a boundary system that separates different security domains, and allows an organisation to enforce its security policy for data transfers between different security domains. Gateways are an important component of a layered cybersecurity defence, and can be shared between multiple organisations, providing the benefits of a common suite of cybersecurity defences. A common use case for gateway deployment is between an organisation's internal network and the internet.

Under the Australian Government's new gateway policy, which includes changes to the PSPF, NCEs are empowered to adopt a risk-based authorisation model. This risk-managed principles-based approach is consistent with the *Information security manual*'s (ISM) principles, and the Government's approach to other cyber architecture and systems, such as the adoption of cloud environments.

The Certification Authority and Accreditation Authority roles for multi-entity Secure Internet Gateways (SIG) in the PSPF are replaced by the risk-based authorisation model for gateways, consistent with authorisation for other ICT systems, with assurance activities conducted by Infosec Registered Assessors Program (IRAP) assessors. ASD's Certification Authority role for multi-tenancy gateways, and ASD's *Certified gateways list*, ceased as of July 2022. This change means NCEs will no longer be required to use ASD-certified gateways, thereby providing them with greater flexibility to use a wider range of gateway solutions that best suit their operating environment and risk appetite.

To support the policy enhancements and the transition to a risk-managed principles-based approach, ASD has co-designed this *Gateway security guidance package* with government and industry representatives from key stakeholder groups through consultative forums.

This guidance takes an objective and principles-based approach to gateways that NCEs can apply, using their risk management framework, to protect their systems and data from cyberthreats. This guidance is not prescriptive to a particular technology or environment given the multi-technology and multi-environment make-up of today's enterprise ICT environments, which include on-premise, cloud and mobile solutions. Instead, it should be interpreted and applied as appropriate to the technology and environment in which services are hosted.

Importantly, this document does not operate in isolation and should be read alongside the relevant and supporting policies applicable to gateways, including the PSPF, the ISM and other relevant ASD guidance.

Introduction

Purpose

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

The purpose of this guidance is to inform decision-makers at the executive level of their responsibilities, the appropriate considerations needed to make informed risk-based decisions, and to meet policy obligations when leading the design, procurement, operation, maintenance and disposal of their organisation's gateway services. This document explains modern gateway technologies and key principles, and provides advice on how to understand and manage risks associated with gateways. This includes the risks of different approaches and guidance on how to use an IRAP report.

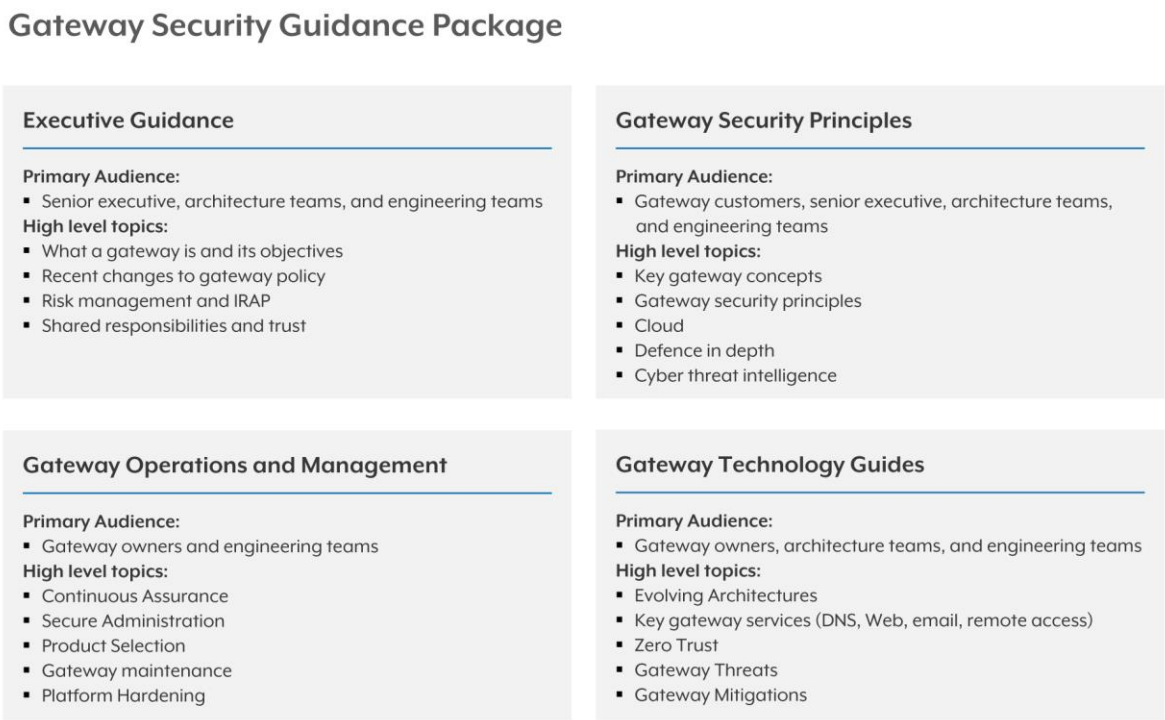
As gateway security functions are becoming readily available in cloud service offerings, gateway architectures are starting to evolve. Hybrid and cloud-native gateway capabilities, combined with new ways of working, will mean that the choice of gateway architectures available to Commonwealth entities is expanding. This guidance package outlines how an organisation should approach the cybersecurity challenges specific to its gateways, noting the availability of flexible and adaptive architectures and delivery models that are now available.

The *Gateway security guidance package* documents should not be considered a policy or checklist, and 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*, *Commonwealth Procurement Rules*, the guidance within the ISM and the PSPF.

Intended audience

This guidance is one part of a package that forms the *Gateway security guidance package*. When designing, procuring, operating, maintaining or disposing of a gateway, it is important to consider all of 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 (NCE) is only used where there may be explicit requirements under the PSPF or other policy.

The threat environment

Malicious cyber activity targeting Australia remains pervasive and diverse. Commonwealth entities are attractive targets to malicious actors due to their holdings of sensitive or classified data, and their provision of critical services to Australia. The substantial shift to remote working during the COVID-19 pandemic also introduced new opportunities for malicious actors to exploit organisations, and new challenges for gateway designers and operators.

ASD has observed malicious actors increasingly focus on targeting 'edge' devices that act as security intermediaries between internal networks and the internet. The rapid use of newly released vulnerabilities is now standard tradecraft for many malicious actors. Both skilled and unskilled malicious actors conduct scanning and reconnaissance against internet-accessible networks to identify unpatched software, and exploit networks that incorporate legacy technologies.

Methods to target Australian networks are constantly expanding and evolving, and this highlights the need to continually strengthen security postures to help mitigate network risks. The *Gateway security guidance package* provides better practice advice on how to configure, monitor and update gateways to improve security and resilience against malicious actors.

ASD continues to provide insights into the cyberthreat environment in the *Annual threat report*.

Background

For the past decade, the Australian Government's SIG policy has determined how gateways are acquired and operated by Commonwealth entities to which the PSPF applies.

In 2019, the Digital Transformation Agency undertook a review of the SIG policy to evaluate potential areas for improvement and modernisation. This guidance aligns with the changes to the PSPF and ISM shifting to a risk-managed principles-based approach for gateways as the outcome of the policy review.

In the past, the Australian Government's Gateway Consolidation Program advocated for the routing of internet traffic through a small number of well-controlled secure internet gateways. These secure internet gateways became the logical place to concentrate cybersecurity capabilities as they controlled all traffic between the trusted internal network and the untrusted internet. This approach created strict rules for system and network architecture and topology.

The availability of modern service delivery and consumption models, such as cloud, software-defined wide area network (SD WAN) and remote work, have highlighted that the traditional monolithic gateway is no longer the only network security model available to Commonwealth entities.

Monolithic gateways, such as SIGs, provide all gateway security functions through one centrally managed system. A disaggregated gateway provides a service-specific gateway function through a discrete system. A hybrid gateway provides all of the gateway services required by an organisation through a combination of monolithic and disaggregated capabilities.

The desire to take advantage of industry trends, such as public cloud services, is impacting the underlying architectures of how these services have traditionally been delivered over the internet. In some cases, data is no longer routed through an organisation's existing gateway or, where it does, it is not in a form that can be readily assessed by existing security tools. As gateway security functions are becoming readily available in cloud service offerings, gateway architectures are starting to evolve. Hybrid and cloud-native gateways, combined with new ways of working, will mean that gateway architectures look different from what they have previously.

What is a gateway?

A gateway is a boundary system that separates different security domains and acts as the first line of defence to provide security capabilities for an organisation and its systems. In doing so, a gateway provides policy enforcement mechanisms for data flows by only permitting data to flow between different security domains in accordance with an organisation's security policy. A common example of a gateway data flow is between an organisation's internal network and the internet.

A gateway is comprised of a collection of physical and logical components that enforce a security policy to manage access to, and transfer of, data from one security domain to another. In a cloud service provider model, or a managed service provider model, a gateway may be abstracted to a set of security services and capabilities that are exposed to consumers.

A gateway should be deployed as a combination of physical and logical components and capabilities that operate collectively as a single integrated solution. All successful gateway solutions align with, and defend, an entity's evolving business requirements.

In isolation, gateways do not provide defence-in-depth, but are an important mechanism in an organisation's cybersecurity strategy. Each organisation is responsible for maintaining the confidentiality, integrity and availability of its data. Cyberthreats can be mitigated through the implementation of controls across a broad range of an entity's information and communication technology (ICT) environment, including by gateways.

For gateways operating at higher Security Classifications, SECRET or TOP SECRET, this guidance should be read alongside ASD's Cross Domain Solution guidance – and solutions designed with evaluated and assessed products where appropriate. Cross Domain Solutions must implement additional services, or require additional monitoring or logging capabilities commensurate with the elevated consequences of unauthorised disclosure of highly classified information.

Gateway design factors

Factors that heavily influence an organisation's gateway design include:

- business and operational requirements and strategies
- technical capabilities
- confidentiality, integrity, availability and privacy requirements
- threat modelling, risk appetite and risk management strategies
- integrations between self-hosted and cloud services
- sourcing and service delivery models
- location and number of data centres and office locations
- availability of staff to design and sustain gateway capabilities.

Regardless of whether a gateway is built and managed in house, outsourced, or provided by a collection of cloud services, it is critical that gateway services and cybersecurity defence capabilities evolve to support an organisation's evolving business and risk management needs.

Objectives of a gateway

A gateway should control the flow of data between security domains and provide visibility of transiting data. As such, it is important that an organisation's gateway stakeholders understand the design principles and objectives of the controls for their gateways. Without understanding the capabilities and limitations of its gateways, an organisation cannot appropriately understand and manage its technical and operational risks.

The core security objectives of a gateway are:

- Visibility – understand and observe data flows
- Detection – monitor for and identify cyberthreats and anomalies
- Prevention – implement controls to enforce security policy on data flows
- Protection – proactively prevent cyberthreats and adequately respond to cybersecurity incidents.

A gateway should meet these security objectives by fulfilling the following functions:

- improve operational and security visibility through the generation of security telemetry
- implement an organisation's risk management policies through technical controls

- reduce attack surface by only permitting approved traffic flows
- enforce security policy:
    - through technical controls implementation
    - through authentication, authorisation and accounting (for specified services)
- prevent breaches of an organisation's security policies
- respond to detected cyberthreats
- enable and protect business services (e.g. web, email and remote access)
- limit or contain the impact of any compromise
- implement compensating controls while suppliers or service provider create and release patches.

What has changed for NCEs?

The changes to the Australian Government's gateway policy aim to create a risk-based authorisation model, consistent with how other ICT systems are authorised to operate. The gateway policy update includes changes to the PSPF that aligns the process for gateways with the existing Authorisation to Operate (ATO) processes as outlined in the PSPF, replacing the previous Certification Authority role performed by ASD and empowering NCEs to adopt a risk-based approach to gateways.

These changes mean NCEs will be provided with greater flexibility to use a wider range of gateway solutions that best suit their operating environment and risk appetite, within a risk-managed principles-based approach.

The high-level objectives of these changes are to:

- enable the use of new gateway technologies and architectures
- support a risk-based model for gateway design and operation
- promote continual assurance and improvement.

At the highest level, gateways should be well governed, provide operational visibility, enforce an organisation's security policy and provide protection from known cyberthreats.

NCEs can choose how they procure or implement their gateway capabilities, provided the gateway:

- sufficiently mitigates cybersecurity risks
- is granted an ATO by an authorising officer
- meets the NCE's security governance requirements
- meets personnel security requirements
- meets physical security and information security objectives as outlined in the PSPF (including supply chain risk management)

- considers the *Gateway security guidance package*.

NCEs can choose to consume gateway services through an existing commercial or government gateway provider; however, these services are no longer certified by ASD. NCEs are encouraged to make use of IRAP and make their own risk-based decision as to the suitability of a gateway provider or solution.

Each NCE that is either building or consuming a gateway service will need to review its IRAP report to verify that the gateway services meet the security and operational requirements of the NCE. Under the new model, an NCE may choose to supplement their existing gateway services with additional services, or may elect to migrate their own gateway services, noting that these services will need to be IRAP-assessed, consistent with the PSPF.

NCEs who consume a gateway service from or through another NCE in multi-tenancy arrangement (considered client entities), will retain responsibility for their own risk management activities.

Australian Government policy applicable to gateways

The PSPF states:

Entities must protect internet-connected ICT systems, and the information and data they process, store or communicate, by implementing a gateway consistent with the Information security manual and the Department of Home Affairs' Gateways Policy.

Australian Government entities procuring gateway services must consider the Department of Home Affairs' *Hosting Certification Framework* (HCF), and ensure all sensitive and classified government data, and associated infrastructure rated at the security classification level of PROTECTED is hosted by an HCF-certified provider.

Gateway security principles

There are a number of governance-related security principles that organisations need to be aware of as part of using gateways. These are:

- risk cannot be outsourced
- security management is continuous
- risk is continuously managed
- the invisible cannot be protected
- gateways protect organisations and staff
- Commonwealth entities have specific obligations
- plan for security flaws
- balance business and security.

Risk management for NCEs

PSPF requirements

The PSPF states that entities must only process, store or communicate information and data on an ICT system that the authorising officer (or their delegate) has authorised to operate based on the acceptance of the residual security risks associated with its operation.

To the extent consistent with legislation, NCEs must apply the PSPF using a security risk management approach when using a gateway, including a gateway service provider, their own systems, or both. An NCE remains accountable for its adherence to the PSPF and this accountability cannot be transferred to a third-party gateway service provider, including another NCE.

This enables an NCE to apply the PSPF in a way that best suits its organisation's security and risk objectives, threat environment and security capability.

Authorisation to operate

The authorising officer (or their delegate) is required to undertake governance processes, as stipulated in the PSPF. This includes granting all systems that process government data an ATO. The Determining Authority must understand the risks associated with using a system, including a review of the gateway system's security documentation.

The ISM's risk management framework

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 cybersecurity.

Broadly, the ISM's risk management framework includes six steps as shown in Figure 1.

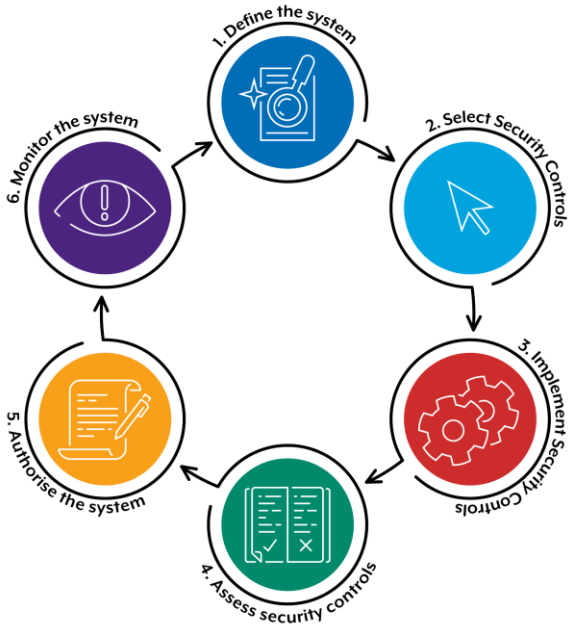


Figure 1: ISM's six-step risk-based approach for cybersecurity

Risk considerations for outsourcing gateway services

An organisation's risk management approach should be used to balance the benefits of a gateway with the security risks associated with the organisation handing over control to a gateway provider. A risk assessment should consider whether the organisation, as a gateway consumer, is willing to trust its reputation, business continuity and data to a gateway provider. Consideration should also be given to the recovery of the consumer's data, should it be insecurely transmitted, stored or processed.

The risks should be weighed against the security capabilities available in-house or available through an outsourced arrangement.

A contract for an outsourced gateway service should address mitigations to governance and security risks, and cover who has access to the consumer's data and the security measures used to protect that data. A gateway provider's responses to important security considerations should be captured in a Service Level Agreement or other contract to ensure that they can be verified and enforced.

In some cases, it may not be possible to independently verify whether a gateway provider is adhering to contracted terms, requiring the consumer to rely on third-party audits. Where visibility gaps occur, a consumer may again need to rely on third-party audits, such as a Security Construction and Equipment Committee (SCEC) or an HCF audit. Consumers should consider which associated documents to request from the gateway provider, and whether the contents of the documents provide the appropriate information to satisfy assurance requirements.

Infosec Registered Assessors Program

Under IRAP, ASD endorses suitably-qualified cybersecurity professionals to provide the relevant services intended to secure broader industry and Australian Government systems and data. IRAP assessors assist in securing an organisation's systems and data by independently assessing the organisation's cybersecurity posture, identifying security risks and suggesting mitigation measures. In all cases, assessors should hold an appropriate security clearance and have an appropriate level of experience and understanding of the type of system they are assessing.

IRAP assessments for gateway

The PSPF has been updated to require security assessments for all gateways used by NCEs to be conducted by an IRAP assessor regardless of the type of gateway (e.g. cloud-provided, multi-tenancy gateway or a service-specific gateway). In line with the policy, a gateway is to be re-assessed at least once every 24 months.

All gateways used by NCEs will need to be IRAP-assessed in their final state, prior to a system being granted an ATO. Where an organisation's operational processes and procedures cannot be verified (e.g. a new system, or where there are Plan of Action and Milestones [POAM] requirements that must be actioned), an authorising officer should consider granting the system ATO with caveats placed on its use, which may include performing the next IRAP assessment earlier than the recommended 24-month interval.

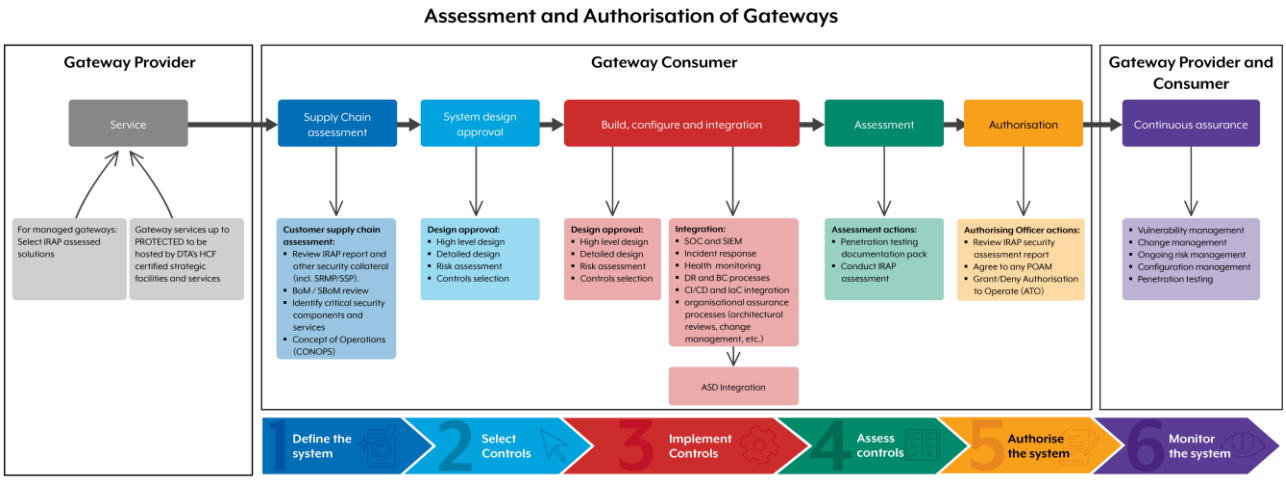


Figure 2: Assessment and authorisation of gateways

NCE considerations for cloud gateway IRAP assessments

Where a cloud-based gateway is developed for an NCE, the organisation designing the cloud gateway should choose a service provider that has already undertaken an IRAP assessment of the services that will be used to perform the gateway functions (known as a Phase 1 assessment). After conducting a supply chain review, the organisation may choose to proceed with building the gateway from these IRAP assessed components.

After integrating the cloud gateway with existing systems, an IRAP assessment of the final state of the gateway system must occur (known as a Phase 2 assessment). The scope of the Phase 2 assessment will include gateway integrations with other operational systems, such as the organisation's authentication systems, Security Information and Event Management (SIEM) and related Security Operations Centre (SOC) integrations, and alignment with the organisation's cybersecurity incident response, disaster recovery and business continuity processes.

Note, to manage conflicts of interest, different assessors should conduct the final state gateway assessment and the cloud service provider assessment.

Preparing for an IRAP assessment

An IRAP assessment is performed against the controls in the ISM as well as other related ASD guidance, such as this guidance. The *IRAP assessment process guide* is a tool for IRAP assessors that details how an assessor should approach and conduct an assessment on a system.

An IRAP assessment will typically involve the review of a number of gateway-specific security artefacts, as well as a number of artefacts relating to a broader range of governance processes of the organisation. This typically includes the following artefacts:

- concept of operations (CONOPS), including a high level design (HLD) or detailed design (DD)
- system security plan (SSP)
- system security plan annex
- cybersecurity incident response plan
- continuous monitoring plan (CONMON)

- cybersecurity incident register
- change management policy
- vulnerability management plan
- standard security clauses in contracts (for service providers)
- standard operating procedures (SOPs)
- corrective actions register
- other gateway security policies and processes.

Note, this list is not exhaustive. An IRAP assessor may request a broader range of an organisation's policy and process documentation.

Service-specific gateway patterns

Where a service-specific gateway pattern is IRAP-assessed and has been granted an ATO by an organisation's authorising officer, subsequent deployments of these patterns within a security domain may be assessed either by an IRAP assessor or an entity assessor. In these cases, the service specific gateway pattern must be managed by the same entity which IRAP assessed the initial architecture. Service-specific gateways deployed in this manner should be under common administrative control, within the same security domain as the initial pattern, with configuration management in place to ensure consistent deployment and configuration (e.g. through automation, continuous integration [CI] and continuous delivery [CD] pipelines, infrastructure-as-code [IaC] or other methods).

Consuming an IRAP assessment

The IRAP assessor will document their findings in an IRAP security assessment report (using ASD's cloud security assessment report template where relevant), which will then be provided to the gateway provider (system owner). The report should in turn be shared by the gateway provider with any consumers of the gateway service, for their own risk management and assurance processes.

The independent IRAP assessment forms the basis of the review by the gateway's consumers. The gateway consumer reviews the security assessment report and, when required, the supporting documentation from the gateway provider. The consumer then determines if the gateway meets its security requirements and risk tolerance, and makes an informed decision to approve the use of gateway services for the consuming organisation. For NCEs, the Determining Authority (or delegate) can grant the gateway ATO on behalf of the consuming NCE. This approval may be caveated that the gateway is used in a pre-defined configuration or has specific requirements, which are documented and form part of the approval evidence generated by the Determining Authority or their delegate.

Continuous risk management

The owners, operators and customers of a gateway should continually document and review risks as part of a recurring assurance governance process. Chief information security officers (CISOs) should work directly with governance boards to ensure that they are receiving the information required to effectively govern their organisation's risk management processes. Risk decisions to bypass security policies should be time-bound in order to trigger a formal review process.

There are two primary frameworks for monitoring risk within the Australian Government:

- ISO 31000:2018, *Risk management – Guidelines* – provides principles, a framework and a process for managing risk. It can be used by any organisation regardless of its size, activity or sector.
- ISO/IEC 27001:2013, *Information technology – Security techniques – Information security management systems – Requirements* – specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organisation.

A shared responsibility model should include the sharing of risk from the service provider to their clients (both managed and unmanaged risk), along with guidance on how clients may manage risk.

Cyberthreat intelligence

Cyberthreat intelligence (CTI) should be leveraged as a security mechanism in gateway environments. Gateways should use reputation and dynamic categorisation services, and should be able to ingest other sources of CTI. CTI can be used to enhance the protection provided by many gateway components, including firewalls, forward and reverse proxies, mail relays, recursive DNS resolvers, and VPN services.

The Cyberthreat Intelligence Sharing (CTIS) Service is ASD's automated cyberthreat intelligence sharing service. This service allows partners to bi-directionally share CTI in a common language via a secure machine-to-machine sharing mechanism. CTI can be shared using a variety of transport layers, including Malware Information Sharing Platform (MISP) and Structured Threat Information Expression (STIX) cyberthreat intelligence via the Trusted Automated eXchange of Indicator Information (TAXII) communications protocol. Access to the CTIS platform requires entities to sign ASD's CTIS Agreement in addition to signing a confidentiality deed and enrolling in ASD's Cybersecurity Partnership Program.

Shared responsibility and trust

The use of managed service providers (MSPs) and cloud service providers (CSPs) requires that organisations place some degree of trust in the service provider, and take steps to ensure that an outsourced service provider is managing risk appropriately.

Gateway security is a shared responsibility between the gateway provider, the gateway consumer and any other third parties who are involved in providing the complete gateway solution, including cloud platforms underpinning gateway services.

Roles and responsibilities

Under the PGPA Act and the PSPF, an NCE's Determining Authority is the identified position responsible for understanding and managing risk within their organisation, and for granting systems an ATO. An organisation's architecture, engineering and operations teams all play an important part in providing information that helps the organisation develop an understanding of its risk profile and the operating threat landscape.

The PSPF and the ISM contain information about formal organisational roles.

As part of using a gateway provider's services, gateway consumers need to understand their own responsibilities, as well as the responsibilities of the other parties involved in delivering the complete gateway solution. This includes understanding each party's responsibilities for securing the gateway; for example, security policy configuration, cybersecurity incident response, data backup, monitoring, security hardening, patching and encryption. In some of these examples, one party may be entirely responsible, or different aspects may be shared between parties.

As part of the IRAP security assessment report for a gateway, IRAP assessors are to document which party is responsible for securing key aspects of each gateway solution in scope of the assessment. This provides gateway consumers with a clear understanding of the different responsibilities that each party has for securing the gateway solution, including their own.

Regardless of the shared responsibility model, gateway consumers remain accountable for their data, including taking steps to ensure the data is appropriately secured.

Organisations should verify that gateway controls are in place, operating effectively, and providing the required visibility and audit. Access requirements should be proportionate to the gateway service, and organisations should only provide MSPs and CSPs with the access required to operate the gateway environments.

Cybersecurity incident reporting

When using a service provider, cybersecurity incident reporting processes should be formalised through a shared responsibility model. For example, if an illegal activity was discovered through a gateway control, both parties should clearly understand how this will be reported to the appropriate authorities. Organisations should consider contractual obligations to report any cybersecurity incident or breach to the gateway consumer.

Early detection of a cybersecurity incident, and timely reporting to the entity's CSO or CISO, is critical to expediting containment and recovery. The PSPF outlines the requirements and obligations of NCEs for the reporting of security incidents, including cybersecurity incidents. See also the ISM's *Guidelines for cybersecurity incidents*.

Both MSPs and their customers will benefit from contractual arrangements that clearly define responsibilities.

- MSPs, when negotiating the terms of a contract with their customer, should provide clear explanations of the services that the customer is purchasing, services that the customer is not purchasing, and all contingencies for cybersecurity incident response and recovery.
- Customers should ensure that they have a thorough understanding of the security services that their MSP is providing via the contractual arrangement, and address any security requirements that fall outside the scope of the contract. Contracts should detail how and when MSPs notify the customer of a cybersecurity incident affecting the customer's environment.
- Customers should ensure that they have trust in the service delivery models provided to them by MSPs and CSPs, particularly with respect to the countries/jurisdictions in which support service teams of MSPs and CSPs may be based.
- Contracts should clearly define sanctions, penalties and exit clauses for not fulfilling contact terms, noting that penalties rarely compensate an organisation for all of the losses incurred as a result of a cybersecurity incident.

The Cloud Security Alliance describes a shared responsibility model as:

In a traditional data centre model, you are responsible for security across your entire operating environment, including your applications, physical servers, user controls, and even physical building security. In a cloud environment, your provider offers valuable relief to your teams by taking on a share of many operational burdens, including security. In this shared responsibility model, security ownership must be clearly defined, with each party maintaining complete control over those assets, processes, and functions they own. By working together with your cloud provider and sharing portions of the security responsibilities, you can maintain a secure environment with less operational overhead.

Further information

Further information on topics covered in this section can be found in the following cybersecurity guidelines.

The *Information security manual* is a cybersecurity framework that organisations can apply to protect their systems and data from cyberthreats. The advice in the *Strategies to mitigate cybersecurity incidents*, along with its Essential Eight, complements this framework.

Further information on CDS is available in the *Fundamentals of Cross Domain Solutions* publication.

Further information on gateway management is available in the *Guidelines for gateways* publication.

Further information on implementing network-segmentation and segregation is available in the *Implementing network segmentation and segregation* publication.

Further information on preparing for and responding to cybersecurity incidents is available in the *Cybersecurity incident response planning: Executive guidance* and *Cybersecurity incident response planning: Practitioner guidance* publications.

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.

Copyright

© Commonwealth of Australia 2022.

With the exception of the Coat of Arms, the Australian Signals Directorate logo and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International licence (www.creativecommons.org/licenses).

For the avoidance of doubt, this means this licence only applies to material as set out in this document.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 licence (www.creativecommons.org/licenses).

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 (www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines).

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

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

Australian Government

Australian Signals Directorate