Hosting Certification Framework (HCF) Application and Readiness Guide

Overview

The HCF Application and Readiness Guide outlines the requirements for applying and achieving certification as a HCF Certified Service Provider. This guide provides a comprehensive summary of the certification requirements and what the Certifications team will be looking for during an assessment. By understanding the requirements in advance, Service Providers can prepare themselves before registering for certification.

The HCF Application and Readiness Guide is not an official assessment matrix or self-assessment tool.

More information on the HCF can be located on the Hosting Certification Framework website.

Application Guide

Eligibility to apply for HCF Certification

The Hosting Certification Framework currently only applies to Data Centre Providers and Cloud Service Providers that provide hosting services directly to Australian government customers. To be eligible to apply for HCF Certification:

Data Centre Service Providers must be able to demonstrate:

- the entire data centre facility is constructed according to the appropriate zone specifications defined in the Protective Security Policy Framework (PSPF); or
- the data centre includes an area (enclave) used for the delivery of Government services that is constructed to the appropriate zone specifications defined in the PSPF and has a discernible perimeter that separates it from the remainder of the data centre.

Cloud Service Providers must be able to demonstrate they only use data centre facilities, or enclaves that are either:

- certified under the HCF; or
- have been fully assessed and considered to satisfy the certification requirements.

Applying for HCF Certification

To register your interest to become certified under the Australian Government's Hosting Certification Framework, please complete the Register your interest form on the Hosting Certification Framework website.

Contract arrangements with Government customers

Service providers that have registered their interest to apply for HCF Certification are able to respond to a market approach or enter contract negotiations for solutions that involve a hosting service component with Australian government customers at the certification level they have registered interest.

Readiness Guide

Category	Requirements
Customer Due Diligence	An approach to due diligence that demonstrates how data is kept separate and secure when housing government and non-government data in the same building. Security arrangements and processes ensure separation of customers areas and restricted access across the facility.
Security Vetting	Assurance that personnel with access to secure areas within the facility and/or government data have relevant security clearances. Security clearance requirements depend on the type of role performed by different personnel. • "Key Personnel with unescorted access to secured areas within a facility, hold an AGSVA recognised security clearance to a minimum of Negative Vetting Level 1. • "Relevant Personnel" with unescorted access to secured areas within a facility, hold an AGSVA recognised security clearance to a minimum of Negative Vetting Level 1. • "Ancillary Personnel" with unescorted access to facilities hold an AGSVA recognised security clearance to a minimum of Baseline. Note: escorting access to secured areas within a facility, requires an AGSVA recognised security clearance to a minimum of Negative Vetting Level 1 and escorting access to facilities requires an AGSVA recognised security clearance to a minimum of Baseline. The Certification's team supports providers to understand how your personnel align with the requirements above.
Ownership	Demonstrate that the majority of the company is owned by low-risk entities. Describe the structure of the company and how parties that control the organisation will exercise decisions consistent with the Commonwealth's interests.
Control, Strategy, and Direction	The company is structured and controlled by individuals and parties that exercise strategic and direction-setting decisions that are consistent with the Commonwealth's interests.
Buildings, Land, and Infrastructure Ownership and Control	Communicate any risks associated with the ownership and control of the buildings, land and core infrastructure that support the facility.
Physical Access Security	Demonstrate how the entire facility, or data halls within facilities that are in scope for certification, are constructed according to the appropriate zone specifications defined in the Protective Security Policy Framework (PSPF). Show how Government data is kept separate from non-government data.
Monitoring Systems	Demonstrate that systems are used to monitor the security and availability of facility operations. An assessment of the risks associated with entities that own monitoring systems.

Category	Requirements
Supply Chain Risk Management	Assurance that foreign entities within your supply chain do not pose risks to the Commonwealth. This includes the supply of critical services such as water, gas, and back-up power. Illustrate how risks are managed in practice through registers and processes.
Highly Secure and Redundant Communications	Demonstrate how the facility manages secure backup systems and business continuity processes in the event of a disaster.
Highly Secure and Suitable Certainty of Supply	Demonstrate how critical infrastructure and services, including water, fuel, gas, and Heating, Ventilation, and Air Conditioning (HVAC), remain resilient in the event of a disaster.
Ancillary Services	Demonstrate that ancillary service providers are owned and controlled by low-risk entities. These services include facility security, cleaning, and technical maintenance are supplied by entities and personnel that do not pose risks to the Commonwealth. Illustrate that personnel provide these services for the minimum time required with restricted access to fulfil their duties.
Remote Support Arrangements	Demonstrate how access and control is managed for remote support workers within and outside of Australia.
Ongoing Compliance	Demonstrate how your company will undertake ongoing compliance with the framework and provide the Commonwealth with continuous assurance through monitoring and reporting.
Relationship to Government	Commitment from the organisation that significant changes, including but not limited to, company ownership, the facility, services, and personnel, will be disclosed in a timely manner.
Exclusive use of Certified Facilities by Cloud Service Providers	Cloud services are hosted in data centre facilities, or zones within a discernible perimeter, that are certified under the framework to the appropriate level.
Data Protection	Demonstrate how data is protected at rest, during processing, and in transit.

HCF quick references

The HCF forms a part of the Australian Government's broader security policy ecosystem. The information sources below may assist providers in understanding the relationship between the HCF and other policies and frameworks.

Resource	Policy owner	Relationship
Protective Security Policy Framework (PSPF)	Home Affairs	Policy 11 of the PSPF: Robust ICT systems, provides the mandate for the HCF.
Information Security Manual (ISM)	Australian Signals Directorate	The ISM is a cyber security framework that agencies can apply, using their risk management framework, to protect their systems and data from cyber threats.
Trusted Information Sharing Network (TISN)	Home Affairs - Cyber and Infrastructure Security Centre	TISN sectors enable critical infrastructure owners and operators to share information on threats and vulnerabilities. The sectors collaborate on appropriate measures to mitigate risk and boost resilience.
Security of Critical Infrastructure (SOCI) and Systems of National Significance (SONS)	Home Affairs	The *Security of Critical Infrastructure Act 2018* was amended in April 2022 to include enhanced cyber security obligations for systems of national significance. The Act includes a category for providers that deliver Data Storage of Processing services as defined under s12F. The definition encompasses assets that are critical to maintaining the supply and availability of data and cloud services located in Australia. To meet the requirements of the Act, providers must develop and maintain a Risk Management Program (RMP). However, providers that are HCF Strategic Certified are exempt from the RMP and are deemed to have fulfilled this requirement through the certification process.
Defence Industry Security Program (DISP)	Defence Information Security Office (DISO)	DISP supports Australian businesses to understand and meet their security obligations. Membership provides the ability for an organisation to sponsor its own security clearances (not available for Entry Level membership). Although the program is primarily for Defence contracts, Home Affairs can liaise with DISO if exceptions are required.
National Data Security Framework (NDSF)	Home Affairs	The framework sets out a long-term vision to create a national ecosystem of data that is accessible, reliable and relevant. It has three main tenets – maximising the value of data, trust and protection, and enabling data use.
The Information Security Registered Assessors Program (IRAP)	Australian Cyber Security Centre	The Information Security Registered Assessors Program (IRAP) produces accredited assessors that conduct independent assessments of a system's cyber security posture. The IRAP risk report can be used as evidence for HCF assessments.
Security Construction and Equipment Committee (SCEC)	Attorney Generals Department	The Security Construction and Equipment Committee (SCEC) is a standing inter-departmental committee responsible for the evaluation of security equipment for use by government agencies. SCEC is also responsible for the SCEC Security Zone Consultant scheme. SCEC reports produced by accredited assessors are required for certification to ensure physical security requirements have been met.

Resource	Policy owner	Relationship
T4 Protective Security	Australian Security Intelligence Organisation (ASIO)	ASIO-T4 provides an ongoing advisory service for government clients and business enterprises. Advice may relate to perimeter security, access control measures, Closed-Circuit Television (CCTV), alarm systems, locks and other door hardware, advice on the construction of new buildings, security zone construction, guarding arrangements, security audits and administrative and personnel security.
Privacy Act	Office of the Australian Information Commissioner	The *Privacy Act 1988* (Privacy Act) was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations with an annual turnover of more than $3 million, and some other organisations, handle personal information. The Privacy Act includes 13 Australian Privacy Principles (APPs), which apply to some private sector organisations, as well as most Australian Government agencies.
Data Availability and Transparency Act 2022	Office of the National Data Commissioner	The *Data Availability and Transparency Act 2022* establishes the DATA Scheme under which Commonwealth bodies are authorised to share their public sector data with Accredited Users. Accredited Users are authorised to collect and use the data, where the requirements of the Act are met. The Act enables the sharing of public sector data consistently and use of appropriate security safeguards.
Department of Foreign Affairs and Trade (DFAT Sanctions List)	Department of Foreign Affairs and Trade	The Consolidated Sanctions List contains all persons and entities listed under Australian sanctions laws. Listed persons and entities are subject to targeted financial sanctions. To meet the “Customer Due Diligence” requirement, Service Providers are required to demonstrate that entities on this list do not have access to facilities.