



Australian Government

Hosting Certification Framework

Draft V2

July 2025

Executive Summary

The HCF provides a standardised approach to security and risk management for DCPs and CSPs handling security classified information and data. It supports the secure management of government systems and information by certifying that hosting and infrastructure services meet consistent and effective risk management standards.

The HCF offers clear and specific guidance to service providers and Non-corporate Commonwealth Entities (NCEs), ensuring only HCF Certified hosting services are used to store, process, and communicate Security classified information and data.

In mitigating supply chain and ownership risks, the HCF reinforces the Australian Government's commitment to safeguarding security classified information and data, and strengthening digital infrastructure resilience.

Contents

About the HCF	5
Purpose	5
Applicability and Scope	5
Structure	7
Control Categories	7
Certification Overview	8
Roles and Responsibilities	10
Application Process	11
Overview of the Deed of Certification	12
Certification Model	12
Monitoring and Compliance	14
Obligations	15
Continuous monitoring	15
Change in Circumstances	15
Renewal, Recertification, and Termination	16
Voluntary termination	16
Non-Compliance and Sanctions	17
Enforcement process	17
Positive Compliance Measures	19
Glossary	20
Appendices	21
Appendix A – Definitions	22
Appendix B – Control Requirements	24
The HCF Controls	25
Appendix C – Relationship to Other Frameworks and Policies	28
Foreign Investment Review Board	28
Protective Security Policy Framework	28
Security of Critical Infrastructure Act	29
Information Security Manual	29
International Organization for Standardisation	29

About the HCF

Purpose

The Hosting Certification Framework (HCF) has been developed to help operationalise the Whole of Government Hosting Strategy. It certifies the security of data centres and associated infrastructure supporting hosting services for Non-corporate Commonwealth Entities (NCEs) and in turn security classified information and data. The HCF provides direction and guidance for:

- The Certifying Authority overseeing the certification of providers (the Department of Home Affairs)
- Data Centre Providers (DCPs) and Cloud Service Providers (CSPs), and
- NCEs procuring service providers and accountable authorities managing Systems of Governance Significance (SoGS).

The HCF standardises security and risk management compliance requirements for DCPs and CSPs that process, store, and communicate security classified information and data. In doing so, the HCF assists NCEs in mitigating supply chain and data centre ownership risks by enabling them to identify and source appropriate hosting and related services.

Applicability and Scope

The HCF provides a standardised approach to managing technology risk at the infrastructure level across the Commonwealth. It delivers assurance to the Australian Government that infrastructure supporting the hosting of security classified information and data is subject to consistent and effective risk management practices (Figure 1).

The HCF applies to all DCPs and CSPs delivering hosting services to NCEs for security classified information and data. In accordance with the requirements of the PSPF, the use of HCF Certified services is mandatory for NCEs requiring hosting services for security classified information and data. NCEs may use uncertified providers to host non-sensitive (OFFICIAL) government and commercial information and data.

The HCF provides the Commonwealth with a consistent approach to managing technology infrastructure risk across all NCEs.



► **Applications**

PSPF directions allow the Commonwealth to apply a consistent approach to application risk management across all NCEs to safeguard Commonwealth systems and data.

► **Platform**

Technology risks relating to software that connects different applications and systems are managed by individual NCEs in accordance with their own risk appetites.

► **Infrastructure**

This layer requires greater oversight and adherence to standards, commensurate with technical and financial risk.

Figure 1: HCF Risk Management Context

Structure

The HCF comprises three core sections:

- **Certification Overview:** Obtaining HCF Certification, and the roles and responsibilities of core HCF stakeholders.
- **Monitoring and Compliance:** Ongoing obligations and responsibilities.
- **Non-Compliance and Sanctions:** HCF compliance enforcement.

s. 33(a)(i), s. 47C(1)

Contact Us

The Department of Home Affairs produces and maintains the HCF.

- Contact Email: hostingcertifications@homeaffairs.gov.au

Certification Overview

HCF Certification is available to all DCPs and CSPs with Australian-based facilities and services seeking to deliver hosting services to the Commonwealth. Upon application, the Certifying Authority will assess the provider's suitability against control requirements outlined in Appendix B – Control Requirements.

The certification process includes an assessment of the underlying hosting services and data centre facilities used to deliver the offering. As a result, certification may be granted for specific services delivered out of specific data centre facility arrangements only, and not necessarily for all facilities or all services delivered by the provider.

HCF Certification confirms that the provider:

- Meets the Commonwealth's minimum security and risk management expectations
- Has no foreseeable changes in strategic directions, operations, or ownership which would adversely affect:
 - Public confidence in the Commonwealth
 - Australian national interests, or
 - The continuity and certainty of services delivered under existing Commonwealth contracts.

HCF Certification does not constitute a guarantee of contract award. Procurement decisions remain subject to Commonwealth procurement rules and NCE-specific requirements.

Providers that do not obtain HCF Certification are considered 'uncertified'. NCEs may engage uncertified providers only where:

- A risk assessment determines it is appropriate to do so, and
- No security classified information or data will be hosted with the provider.

An overview of the HCF certification lifecycle is provided in Figure 2 below.

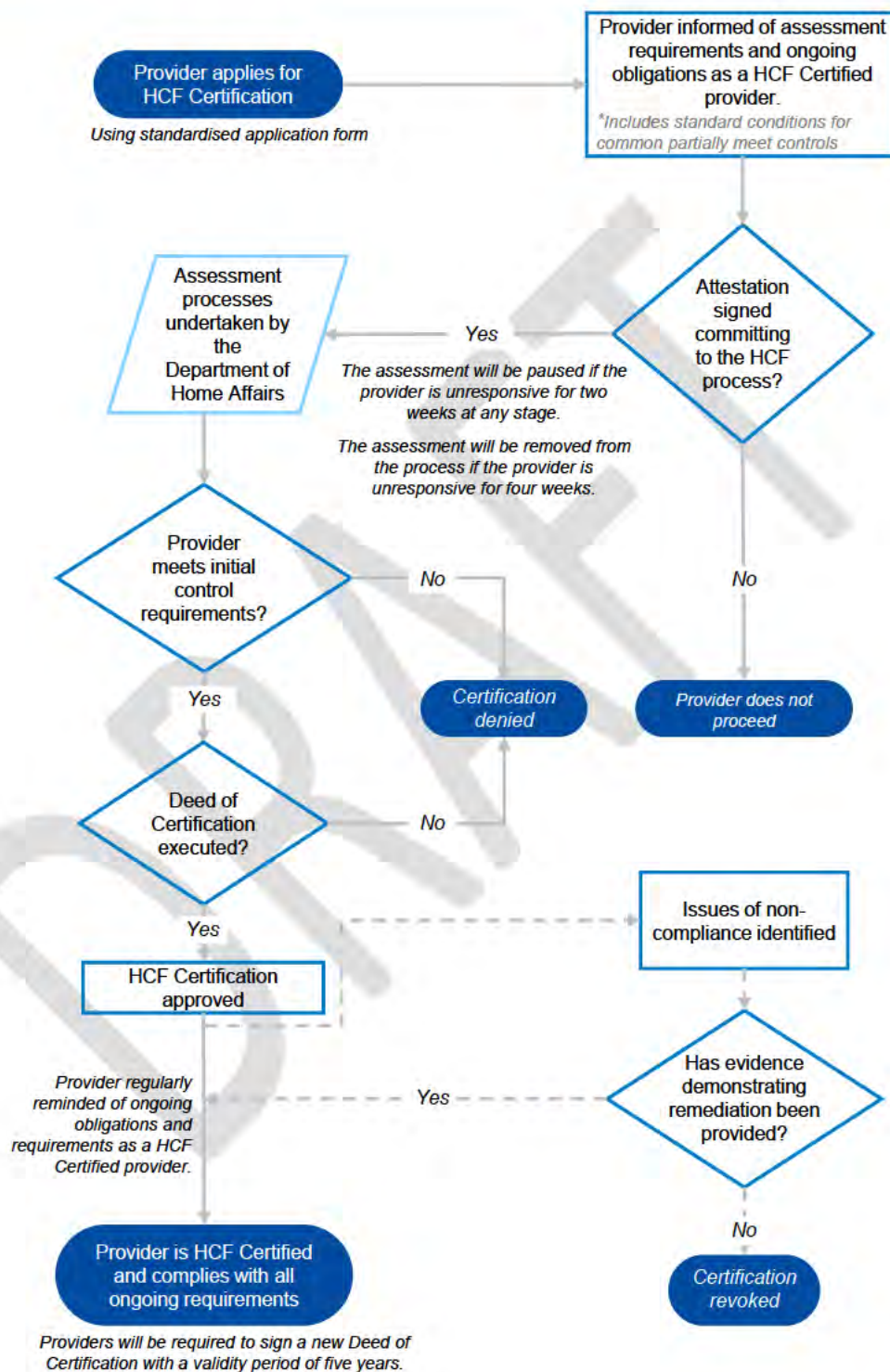


Figure 2:1 HCF Certification Lifecycle

Roles and Responsibilities

To ensure transparency, accountability, and effective governance throughout the HCF Certification lifecycle, responsibilities are clearly delineated across the key stakeholders.

HCF's key stakeholders are the Certifying Authority, NCEs, service providers, and Technical Authority Entities, and roles and responsibilities of each group are demonstrated in Table 1 below.

These responsibilities are mapped using the RASCI model, a structured framework which defines who is Responsible, Accountable, Supporting, Consulted, and Informed at each stage of the certification process.

- **Responsible (R):** The entity responsible for completing the work
- **Accountable (A):** The entity ultimately answerable for the outcome
- **Supporting (S):** The entity providing resources or assistance
- **Consulted (C):** The entity whose input is sought before a decision or action, and
- **Informed (I):** The entity who is kept up to date on progress and decisions.

Task / Entity	Certifying Authority	NCEs	Service Provider	Technical Authority Entities
Application submission and providing required information	S/C	I	R/A	I
Completing the assessment process	R/A	I	S/I	C
Finalising assessment results and confirming HCF Certification status	R/A	I	I	C
Submission of ongoing assurance and compliance reporting	A	I	R	I
Compliance monitoring and review	R/A	I	I/S	C
Conduct of audit and assurance activities	R/A	I	S	C
Procurement/Pre-procurement Risk Assessments	I/S	R/A	S	I
Selecting when to use HCF Certified services	S	R/A	C	I

Table 1: HCF Roles and Responsibilities

Application Process

Providers seeking HCF Certification must submit an application via the Hosting Certification Framework website. This form collects baseline information required by the Certifying Authority to assess the provider's suitability against HCF control requirements, including:

- Provider details, including contact information, and relevant Australian Securities and Investments Commission (ASIC) and Australian Business Register (ABR) information
- Description of the service for which certification is sought
- Foreign Ownership, Control, or Influence (FOCI) information, including details of any critical foreign partners and/or suppliers
- Any current or potential upcoming Commonwealth contracts
- Highest security classification of information to be processed
- Physical locations used to provide the service, including Security Construction and Equipment Committee (SCEC) reports and/or Defence Directorate of Security Assurance (DoSA) accreditation reports
- Infosec Registered Assessors Program (IRAP) reports, and
- Executive-level attestation confirming the accuracy of all information provided at the time of application and a formal commitment to comply with the requirements and obligations of the HCF assessment process.

Overview of the Deed of Certification

As a condition of HCF Certification, providers who progress through the assessment process are required to execute a legally binding Deed of Certification (the Deed). The Deed reinforces the Commonwealth's commitment to secure, resilient, and accountable hosting arrangements, and ensures that HCF Certified providers remain aligned with evolving national security expectations.

The Deed formalises the provider's certification status, reinforcing their alignment with the Commonwealth's security and risk management expectations. This provides a clear signal to NCEs that the provider is a trusted and compliant hosting partner, giving NCEs confidence that their security classified information and data will continue to be protected in accordance with Commonwealth security requirements.

Additionally, it provides a contractual safeguard that allows NCEs to terminate existing hosting arrangements with associated costs to be reimbursed by the provider should there be:

- A change in the Commonwealth's risk appetite, or
- A material change in the provider's circumstances (for example ownership, control, or operational posture) that renders the service unsuitable for hosting security classified information and data.

The Deed is valid for a period of five years from the date of execution. To maintain HCF Certification beyond this period, providers must re-execute the Deed upon expiry. Failure to do so will result in the termination of HCF Certification.

Certification Model

HCF Certification certifies specific services delivered out of specific facilities. This approach ensures certification outcomes are precise, risk-informed, and aligned with the Commonwealth's protective security expectations.

In addition to service and location specific assessments, the HCF incorporates entity-level evaluation to address broader provider-level control categories, such as FOCL. This layered model enables a comprehensive assessment of the provider's risk posture and operational environment.

Where a provider has already achieved HCF Certification for a service, subsequent services may be eligible for an expedited Certification process. The ability to use and speed of any expedited process is contingent on the recency and relevance of prior provider- and location-level assessments, and whether they remain acceptable within the Commonwealth's current risk appetite.



To ensure proportionality and consistency, HCF Certification is tiered based on the highest security classification of information or data the service is intended to process or store, with defined minimum baseline controls that all providers must meet regardless of classification level (outlined in Appendix B – Control Requirements).

This model (illustrated in Figure 3) ensures:

- Security classified information and data is protected in a manner commensurate with its classification and associated risks
- Security classified information and data is processed and stored in accordance with the requirements of the PSPF and the ISM, and
- Hosting environments are appropriately aligned with the Commonwealth's expectations for maintaining the confidentiality, integrity, and availability of information and data assets.

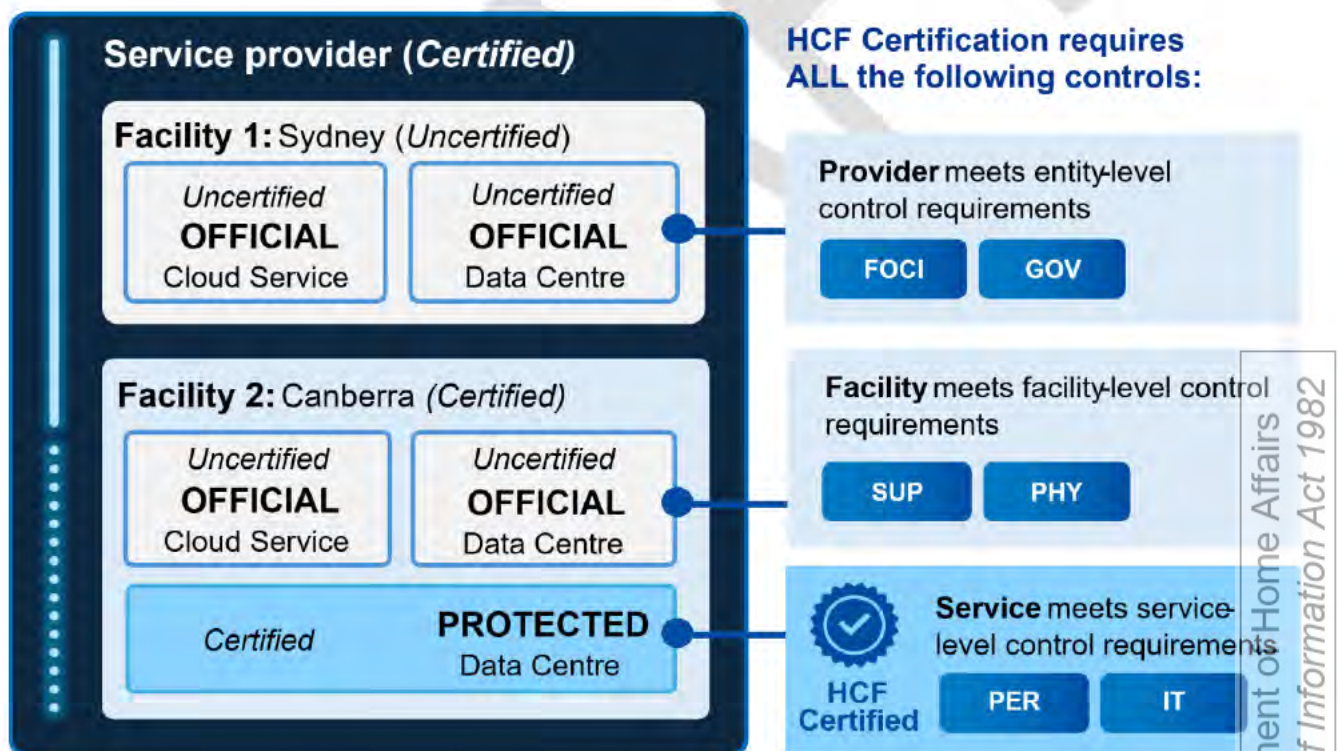


Figure 3:2 Example Application of HCF Certification Model

Monitoring and Compliance

To uphold the integrity and effectiveness of the HCF, a structured set of oversight and assurance mechanisms is embedded within the certification lifecycle. These mechanisms are designed to ensure that HCF Certified providers continue to operate in alignment with the Commonwealth's protective security expectations and maintain a security posture commensurate with the sensitivity of the data and services they support. This enables the Department of Home Affairs to monitor implementation, identify vulnerabilities, and respond to emerging risks in a timely and coordinated manner.

The three core compliance mechanisms are:

1. **s. 33(a)(i), s. 47C(1)**
2. **Periodic Spot Audits:** HCF Certified service providers must notify the Certifying Authority of all contractual arrangements with NCE customers. The Certifying Authority will conduct periodic audits informed by a risk-based assessment of the criticality and business impact of the security classified information and data hosted by the service provider. These audits form part of the broader compliance monitoring framework and provide assurance that certified providers continue to meet their obligations under the HCF.
3. **Enhanced Security Incident Reporting:** HCF Certified service providers are subject to broader reporting obligations than those required under the *Security of Critical Infrastructure Act 2018* (SOCI Act). While SOCI requires reporting on direct impacts to critical infrastructure assets, the HCF requires providers to report any incident that affects the confidentiality, integrity, or availability of systems or data used to deliver the HCF Certified service. This includes incidents arising from supply chain dependencies or third-party services that may disrupt service delivery, as well as any security event that could impact the Certification status of the HCF Certified service. Security incidents that fall outside SOCI thresholds must be reported to the Certifying Authority as soon as practicable within 72 hours, or within 12 hours if the incident is assessed as critical.

Obligations

Continuous monitoring

s. 33(a)(i), s. 47C(1)

As part of the Annual Assurance Reporting process, providers must submit an attestation signed by a director-level executive or higher, confirming the provider remains compliant with all HCF controls and has disclosed any material changes in circumstances, including the initiation or termination of contracts with NCEs.



Change in Circumstances

s. 33(a)(i), s. 47C(1)

Renewal, Recertification, and Termination

In addition to Annual Assurance Reporting, HCF Certified service providers are required to execute the Deed, which remains valid for a period of five years from the date of certification. This validity period aligns with the typical duration of contractual arrangements between certified providers and NCEs, and ensures that providers remain subject to a consistent set of obligations throughout the certification term. The Deed is a mandatory element of the recertification process and must be renewed upon its expiry to maintain HCF Certification status.

Voluntary termination

HCF Certified providers may elect to voluntarily terminate the HCF certification of a service prior to the expiry of the Deed. In such cases, the provider must notify the Certifying Authority by contacting hostingcertifications@homeaffairs.gov.au and providing a rationale for the decision. Voluntary termination must be managed in accordance with the PSPF, ensuring that:

- The termination does not compromise the Australian government's security classified information and data
- Appropriate transition arrangements are in place to maintain continuity of service for affected NCEs, and
- Any residual risks are identified and mitigated in consultation with the Department of Home Affairs.

Following voluntary termination, the provider's certification status will be formally revoked, and the provider will be reclassified as uncertified. NCEs must reassess any ongoing hosting arrangements with the provider in accordance with their risk management obligations.

Non-Compliance and Sanctions

HCF Certified service providers that fail to comply with the requirements of the HCF will be subject to the enforcement process, which may result in the suspension or revocation of HCF Certification.

Enforcement process

For HCF to provide a high level of compliance to NCEs, a graduated compliance enforcement process is in place. This process is triggered when instances of non-compliance are identified.

When an issue of non-compliance is identified, the service provider is initially notified via an informal note of concern, allowing the provider to address the issue. If the service provider does not supply evidence of in-progress or complete remediation of the issue within 20 business days, the formal compliance enforcement process may be initiated.

The enforcement process comprises four core phases (detailed in Figure 4):

1. **Note of concern:** Non-compliant providers receive an informal note of concern outlining the issue of non-compliance. The provider is made aware that if evidence is not provided to demonstrate in-progress or complete remediation within 20 business days, a formal warning will be issued.
2. **Warning:** Non-compliant providers receive a written warning and have 20 business days to show evidence of resolving the issue.
3. **Suspension:** If there is no response or resolution progress within 20 business days of the warning, HCF Certification is suspended, NCEs are notified, and the provider is barred from taking on new contracts.
4. **Revocation:** If compliance or evidence of resolution progress is not provided, Certification may be revoked at the discretion of the Certifying Authority and the Deed terminated, based on a risk assessment of the non-compliance. NCEs will be informed, and the provider must re-apply to regain Certification.

Each phase of the enforcement process allows 20 business days for a response before moving to the next, giving providers a total of 60 business days before HCF Certification is suspended.

In extreme cases, the Certifying Authority may consider options to fast-track the revocation of a service provider's Certification. This instrument will be used as a measure of last resort following significant changes to the Commonwealth's risk appetite, changes in the service provider's circumstances, threat environment, or evaluated risk.

s. 33(a)(i), s. 47C(1)

Each phase of the enforcement process allows 20 business days for a response before moving to the next, giving providers a total of 60 business days before certification is suspended.

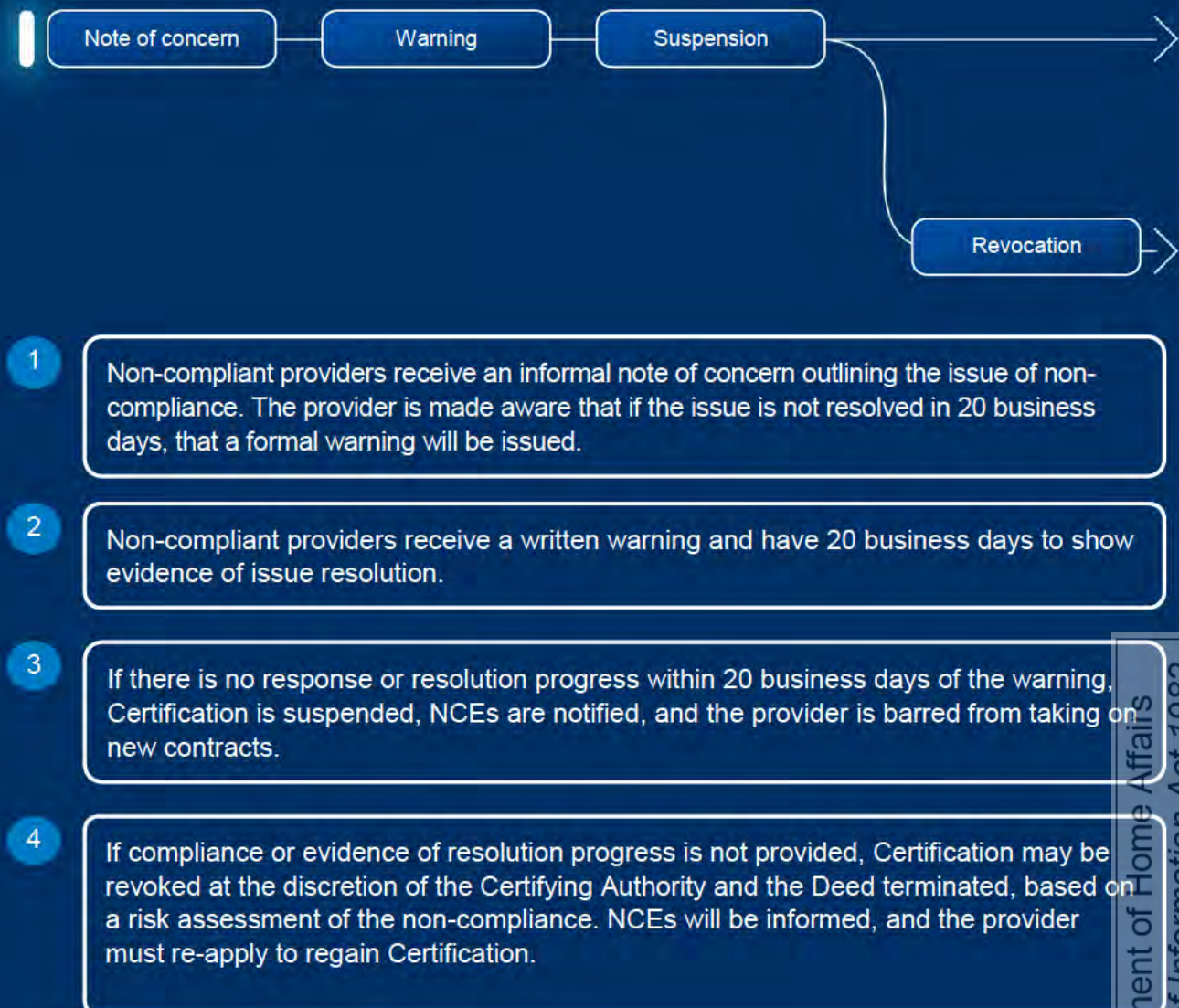


Figure 4:3 HCF Certification Compliance Enforcement Process

Positive Compliance Measures

In addition to formal certification requirements, the HCF incorporates a range of supplementary measures designed to encourage and reinforce positive compliance behaviours among certified providers. These measures operate outside the core regulatory framework and are intended to support a culture of continuous improvement and proactive alignment with Commonwealth expectations.



Glossary

Abbreviation	Meaning
ABR	Australian Business Register
ASD	Australian Signals Directorate
ASIC	Australian Securities and Investments Commission
CSP	Cloud Service Provider
DCP	Data Centre Provider
DoSA	Defence Directorate of Security Assurance
FIRB	Foreign Investment Review Board
FOCI	Foreign Ownership, Control and Influence
GOV	Governance
HCF	Hosting Certification Framework
ISM	Information Security Manual
ISO	International Organization for Standardization
IT	Information Technology
IRAP	Infosec Registered Assessors Program
NCE	Non-corporate Commonwealth Entity
OT	Operational Technology
PER	Personnel Security
PHY	Physical Security
PSPF	Protective Security Policy Framework
RASCI	Responsible, Accountable, Supporting, Consulted, and Informed
SCEC	Security Construction and Equipment Committee
SOCI Act	Security of Critical Infrastructure Act 2018

Appendices

A – Definitions

B – Control Requirements

C – Relationship to other frameworks

Appendix A – Definitions

A list of defined common and complex terms used in the HCF and HCF control requirements.

Term	Definition
Technology Infrastructure	The servers, storage systems, networking devices, facilities, and related services that deliver IT operations.
Platforms	The software, databases and data management systems, that serve as the foundation for developing and running applications,
Technical Authority Entities	Technical Authority Entities are entities that have additional accountabilities to provide domain-specific security advice, technical standards or intelligence services in support of Australian Government protective security outcomes.
Control	An entity is in a position to directly or indirectly control a second entity if: • The entity is in a position to exercise voting or veto rights in relation to the body that governs the second entity, or • The entity is in a position to make decisions that materially impact on the operational, financial, or strategic policies or direction in relation to the second entity, or • The entity has the ability to appoint: ○ Persons to the body that governs the second entity, or ○ Key personnel involved in the operations of the second entity, or • The entity is in a position to influence or determine decisions relating to: ○ The business plan, or any other management plan, for the second entity, or ○ Major expenditure relating to the second entity, or ○ Major contracts or transactions involving the second entity, or ○ Major loans involving the second entity.
Core Infrastructure	Telecommunications, electricity, water, fuel, gas, HVAC, and backup power services used to support relevant data centre and cloud services.
Ancillary Service Provider	Providers of cleaning, security, technical, and maintenance services.

Term	Definition
Changes in Circumstances	Changes in Circumstances include: • A change in board, management team, personnel or subcontractors • A change in strategic direction, ownership, shareholder arrangements, financial position, NCE contracts or operations • A change in security measures or procedures • A sale or disposal of Australian land • Any transfers, assignments or disposals of any lease or real-estate • Changes to a service provider's supply chain or service dependencies • Security, resilience, and availability incidents, including in supply chain or service dependencies • Changes in service delivery architecture • Majority interest purchases, and • Any other circumstance that may adversely affect security or operations.

Appendix B – Control Requirements

s. 33(a)(i), s. 47C(1)

Released by Department of Home Affairs
under the *Freedom of Information Act 1982*

The HCF Controls

The following mandatory controls apply under the HCF:



Foreign Ownership, Control or Influence (FOCI)

Control #

Control
Sub-Category

Control Statement

s. 33(a)(i), s. 47C(1)



Supply Chain (SUP)

Control #

Control
Sub-Category

Control Statement

s. 33(a)(i), s. 47C(1)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

**Personnel Security (PER)****Control #****Control
Sub-Category****Control Statement**

s. 33(a)(i), s. 47C(1)

**Physical Security (PHY)****Control #****Control
Sub-Category****Control Statement**

s. 33(a)(i), s. 47C(1)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

**Information Technology (IT)****Control #****Control
Sub-Category****Control Statement**

s. 33(a)(i), s. 47C(1)

**Governance (GOV)**

Governance controls are not assessed as part of the initial HCF Certification process. Compliance with these controls is required to maintain HCF Certification.

Control #**Control
Sub-Category****Control Statement**

s. 33(a)(i), s. 47C(1)

Released by Department of Home Affairs
under the Freedom of Information Act 1982

Appendix C – Relationship to Other Frameworks and Policies

The HCF operates as an integral component of the Australian Government's protective security ecosystem. It is designed to support existing security and regulatory frameworks, ensuring a consistent approach to safeguarding security classified information and data.

Foreign Investment Review Board

The FIRB supports the Treasurer in administering Australia's foreign investment framework, which includes the *Foreign Acquisitions and Takeovers Act 1975*, the *Foreign Acquisitions and Takeovers Regulation 2015*, and the Foreign Investment Policy.

FIRB assesses foreign investment proposals against the national interest, considering factors such as national security, market competition, economic impact, and the character of the investor. The Treasurer may approve, reject, or impose conditions on investments to mitigate national interest risks. The HCF aligns with FIRB's objectives by ensuring that hosting providers under foreign ownership or control are appropriately scrutinised. FIRB may also be leveraged to provide information on notifiable changes under foreign investment policy.

Protective Security Policy Framework

The PSPF prescribes minimum security requirements for safeguarding NCEs' people, information, and assets. It provides a structured approach to identifying and managing security risks across six domains: Governance, Risk, Information, Technology, Personnel, and Physical.

The HCF supports the PSPF by ensuring that hosting providers storing security classified information and data meet consistent infrastructure-level security standards.

Security of Critical Infrastructure Act

The SOCI Act establishes a legislative framework to protect Australia's critical infrastructure from threats that may compromise national security, economic stability, or public safety.

The SOCI Act applies to 11 designated critical infrastructure sectors, including data storage and processing, which encompasses DCPs and CSPs.

Under the SOCI Act, entities that own, operate, or have direct interests in critical infrastructure assets are subject to specific legal obligations. These include risk management, mandatory reporting, and cooperation with the Australian Government in the event of a significant incident affecting the security or functionality of a critical infrastructure asset.

As data storage and processing is a defined critical infrastructure sector, DCPs and CSPs may have existing obligations under the SOCI Act. These obligations operate in parallel with HCF requirements. The HCF's FOI controls align with the SOCI definitions of 'control', and security incident reporting requirements are consistent with those mandated under SOCI.

Information Security Manual

The ISM, developed by the Australian Signals Directorate (ASD), provides guidance on securing information technology (IT) and operational technology (OT) systems, applications, and data. It outlines cyber security principles and controls that support risk-based decision-making and compliance with national security standards.

The HCF supports the ISM by requiring hosting providers to align with and implement appropriate technical controls to safeguard security classified information and data, and to demonstrate their effectiveness through IRAP assessments.

International Organization for Standardisation

The International Organization for Standardization (ISO) develops globally recognised frameworks that support consistent, risk-informed security and risk management practices. ISO 28001 provides guidance on supply chain security, while ISO 31000 outlines principles for enterprise risk management.

The HCF supports these standards by requiring hosting providers to implement aligned risk management practices that enhance resilience, support secure service delivery, and safeguard security classified information and data.