Australian Government
Digital Transformation Agency

Whole of Government Hosting Strategy

Hosting Certification Framework

March 2021

dta

Digital Transformation Agency

Version: 1801

Contents

Background

Purpose

The Government has made significant investments in safeguarding the security and privacy of government held data. Cornerstones of this investment include the secure environment of data centres and associated infrastructure that provide hosting services for Australian Government agencies.

The Hosting Certification Framework (the Framework) has been developed to operationalise the principles outlined in the Whole of Government Hosting Strategy (Hosting Strategy) and to support the secure management of government systems and data.

The Framework will assist agencies to mitigate against supply chain and data centre ownership risks and enable them to identify and source appropriate hosting and related services.

Terminology

During consultation undertaken while developing this Certification Framework, it became apparent that the original terminology used in the Hosting Strategy to describe the two levels of certification would benefit from additional clarity.

In particular, the term s*overeign* was taken as excluding any level of foreign investment or control in a hosting provider. Under such an interpretation, given the potential for a level of foreign investment, any publicly listed hosting provider would be ineligible for the higher level of certification. In addition, any privately owned hosting provider would find itself constrained in terms of future growth options that may have exposure to foreign investment.

For clarity, *sovereignty* refers to the ability of the government to specify and maintain stringent ownership and control conditions. The highest level of certification is intended to only be available to hosting providers that meet the stringent assessment threshold of suitability and enable the Government to specify and enact ownership and control conditions that are not lowered at any time.

For ongoing clarity, the terminology for the certification levels has been revised to:

Certified Strategic Hosting Provider *represents the highest level of assurance and is only available to providers that allow the Government to specify ownership and control conditions.*

Certified Assured Hosting Provider *arrangements safeguard against the risks of change of ownership or control through financial penalties or incentives, aimed at minimising transition costs borne by the Commonwealth should a data centre provider alter their profile.*

There has been no change to the scope or threshold of assessment required for hosting providers to become certified at either of the two levels.

Framework Scope

The Framework will apply to all direct and indirect providers of hosting and related data centre services to government customers, including the facilities that host government data, their systems and their supply chains.

Direct and Indirect Providers

Hosting providers under this Certification Framework may be direct or indirect. Direct hosting providers are those contracted by agencies through the current Data Centre Facilities Supplies Panel (Panel 2) administered by the Digital Transformation Agency (DTA).

Hosting providers may also be indirectly providing services to agencies by hosting data and systems through a direct commercial arrangement with a related or third party that has a contractual arrangement with government agencies, such as a systems integrator, a managed service provider or a cloud service provider.

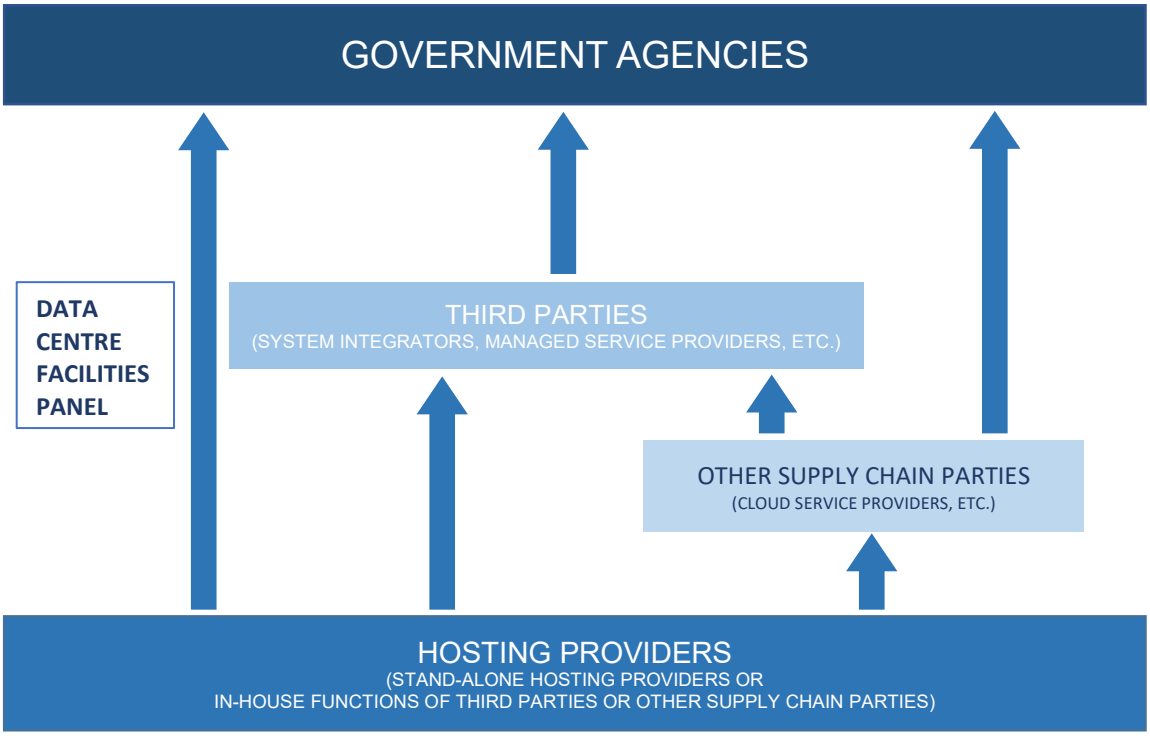

Figure 1 Provision of Hosting Services

Hosting Services

The fundamental service provided by hosting providers to agencies is space in data centre facilities divided into segregated and secured data halls, including physical access security to this space.

The hosting providers also supply the core infrastructure (e.g., generators, electrical power and management of climate control through cooling and ventilation) to ensure the ongoing operation of the environment occupied by tenants.

In some cases, the hosting provider may also provide telecommunications infrastructure across multiple data centre facilities, or between data centre facilities and customers.

In the case of managed service and cloud service providers, these providers may deliver a range of services to agencies that leverage services provided by different hosting providers or third parties. In some cases, the hosting services are provided as in-house functions.

When applied to system integrators, managed service or cloud service providers, the Framework will include an assessment of the underlying hosting services and data centre facilities that are used. As a result, certification of system integrators, managed service and cloud service providers will occur for each data centre facility arrangement used by the provider. This may result in a certification being granted for only some, but not all data centre facilities arrangements utilised by the provider.

In such cases, providers will only be able to use the certified data centre facilities (certified data centre facilities arrangements) that satisfy the certification level required by agencies.

Knowledge of Data and Systems

Whilst hosting providers maintain data centre facilities and act as the landlord for their tenants, hosting providers typically only have access to the equipment (cabinets, racks etc.) in emergency circumstances. They do not have any knowledge of the type and sensitivity of the data hosted by its customers.

In circumstances where the hosting services are provided to agencies indirectly, as in-house functions of systems integrators, managed service providers and cloud service providers, additional risk mitigation measures will be put in place to account for the fact that these service providers will have both knowledge of, and responsibility for, the type and sensitivity of the data hosted by agencies.

Core and Supply Chain Capabilities

Hosting providers develop and rely on core and supply chain capabilities in order to provide services to customers.

While there is some variation between hosting providers as too which core capabilities they develop and which capabilities they source as part of their supply chain, for the purposes of certification, the Framework requires that hosting providers have a minimum set of core capabilities as per Table 1 below. These minimum core capabilities are subject to ownership and control provisions.

The core capabilities have been defined to identify a situation where a hosting provider entering into certification does not have ultimate control or ownership over the core capabilities underpinning the services it is providing.

In such situations, gaining certification may require the ultimate owners of core capabilities to also agree to ownership and control provisions.

Core Capabilities	Subject to ownership and control provisions
Land Ownership	✓
Data Centre Facility Assets/Buildings Ownership	✓
Core Infrastructure Ownership (generators, electrical power and management of climate control through cooling and ventilation)	✓
Physical Access Security	✓
Data Centre Facility Monitoring Systems	✓

Table 1: Core Capabilities subject to ownership and control provisions

In contrast with the minimum core capabilities identified above, other capabilities are deemed as minimum supply chain capabilities, as per Table 2 below. Supply chain capabilities will be subject to security and risk assessments, as opposed to control and ownership provisions.

Supply Chain Capabilities	Subject to security and risk assessments
Telecommunications networks	✓
Providers of critical goods and services (such as water and fuel, data centre core infrastructure and access control, and monitoring systems)	✓
Providers of ancillary services and personnel (such as cleaners, security personnel, technicians, maintenance personnel)	✓

Table 2: Supply Chain Capabilities subject to Security and Risk Assessments

In cases where hosting providers are providing some of the supply chain capabilities as in-house functions i.e., as with the core capabilities, the security and risk assessments will take into consideration the increased degree of ownership and control over these functions.

Relationship to Other Frameworks and Policies

This Certification Framework works in conjunction with a suite of other government policies and frameworks, including Australia's Foreign Investment Policy, the Protected Security Policy Framework, and the provisions protecting Critical Infrastructure and Systems of National Significance.

Foreign Investment Review Board

The Foreign Investment Review Board (FIRB) is a non-statutory body that provides advice to the Treasurer and the Government on Australia's Foreign Investment Policy and its administration. In Australia, foreign investment is regulated by a framework that includes the *Foreign Acquisitions and Takeovers Act 1975* (FATA), the *Foreign Acquisitions and Takeovers Regulation 2015* (the Regulation) and the Foreign Investment Policy.

In considering whether investment proposals are contrary to the national interest, FIRB will consider factors such as national security, competition, other Australian Government policies, the impact on the economy and community, and the character of the investor. The FIRB provides advice to the Treasurer who has the ability to prohibit or impose conditions on investments found to be contrary to the national interest.

The Certification Framework works in conjunction with FIRB and allows Commonwealth agencies to leverage the contractual protections and safeguards applicable under the certification model to respond to a condition imposed by the FIRB (for a notifiable change), or in the case of a non-notifiable change, work with the FIRB to react to a change in circumstance that is not in the Commonwealth interest. By obtaining continuous insight into the strategic direction, ownership, operation and supply chains of providers under the Framework, working with FIRB and enacting the contractual protections the Framework provides, the Commonwealth has an effective

control regime that mitigates the risk, expense and impact of undesirable changes affecting providers.

Protective Security Policy Framework

The Protective Security Policy Framework (PSPF) assists Australian Government entities to protect their people, information and assets, both at home and overseas. It sets out government protective security policy and supports entities to effectively implement the policy considering security governance, information security, personnel security and physical security. Consistent with the approach taken to implementing the Certification Framework, the PSPF is applied through a security risk management approach, with a focus on fostering a positive culture of security within an entity and across the Government.

The PSPF describes the roles and responsibilities of Accountable Authorities and others with security responsibilities, including the requirements and guidance for planning, managing, monitoring and reporting on protective security.

In addition, it details how Accountable Authorities correctly assess the sensitivity or security classification of their information and adopt marking, handling, storage and disposal arrangements that guard against information compromise. Based on the assessed sensitivity or security requirements, the Certification Framework allows Commonwealth agencies to make informed decisions on the certification level of the provider required to appropriately host their information assets.

Protecting Critical Infrastructure and Systems of National Significance

The Certification Framework will also work in conjunction with the powers and provisions of the Government's 2020 Cyber Security Strategy, including those regarding protecting Critical Infrastructure and Systems of National Significance (CI/SoNS), and once legislated, those provisions stipulated in the Security Legislation Amendment (Critical Infrastructure) Bill 2020, which was introduced into Parliament on 10 December 2020.

Development and Collaboration

The Framework has been developed with reference to existing guidelines and reference points, in particular:

- Whole-of-Government Hosting Strategy
- Australian Government Protective Security Policy Framework (PSPF)
- Information Security Manual (ISM)
- Public Governance, Performance and Accountability Act 2013 (PGPA Act)
- Department of Treasury – Foreign Investment Review Board (FIRB), Foreign Acquisitions and Takeovers Act 1975 (FATA Act), and Foreign Acquisitions and Takeovers Regulation 2015
- Commonwealth Procurement Rules, and
- The Department of Home Affairs – Protecting Critical Infrastructure and Systems of National Significance.

The Certification Framework was developed with input from stakeholders, including:

- input from Commonwealth agencies to assess related initiatives such as critical infrastructure assessments
- user research with Commonwealth agencies on current and anticipated needs, and
- industry providers to determine current and planned data centre services.

Implementation

Implementation Approach

Subject to the transition arrangements described below, certification under this framework will take place in a staged approach to ensure that the largest footprint of government systems and data will reside in certified facilities in a timely fashion.

In the first phase, all hosting providers on the Data Centre Facilities Supplies Panel (Panel 2) that are providing services directly to government agencies are eligible to apply for certification under the Framework.

Other parties that host government systems and data as part of providing services (such as systems integrators, managed services providers and cloud services providers) will be able to apply for certification in a second phase of the Framework's implementation.

Additional risk mitigation measures will be put in place in these cases to account for the fact that the services provider have both the knowledge and responsibility for the type and sensitivity of the data hosted by its customers.

The proposed indicative timeline for the certification of providers is provided below:

Phase	Time	Scope
Phase 1	Mar 2021 onwards	All providers can register their interest to apply for a specific certification level.
	Apr 2021 – May 2021	Registered providers Panel 2 are eligible to apply for certification.
	Apr 2021 – Dec 2021	Certification process for Panel 2 providers.
	Sept 2021 – Oct 2021	Other registered providers are eligible to apply for certification as part of Phase 2.
	Nov 2021 – Dec 2021	Certification Framework Review.
Phase 2	Jan 2021 – Jun 2022	Certification process for other providers.

Table 3 Proposed certification timeline

The proposed certification timeline above will be assessed based on demand and will be updated as necessary, with the goal of achieving certification of all registered providers in a timely fashion.

Transition Arrangements

From 1 March 2021, agencies going to market or seeking to enter into a contract for any solutions that involve a data centre component, whether direct or through a third-party provider, must stipulate their requirements for Certified Strategic or Certified Assured Hosting Providers as appropriate.

Providers, including direct and indirect providers, that have registered their interest to apply for a specific certification level will be able to respond to a market approach or enter contract negotiations for solutions that involve a hosting service component at the certification level they have registered interest.

Should a registered provider be selected as the preferred tenderer, the agency will work with the DTA to support expediting the process of certification for that provider.

The Agency will only be able to enter into a contract with the preferred provider if the provider achieves certification at the required level.

Agency Responsibilities

Agencies will continue to have the autonomy to select the best hosting arrangements for their requirements and will be responsible for implementing appropriate data protection controls to comply with the Protective Security Policy Framework (PSPF) and Information Security Manual (ISM). This will also include compliance with the requirements of the Hosting Strategy, such as:

- when considering a hosting solution, agencies must assess data and systems for the likelihood of data sensitivity changing over time; and
- PROTECTED and whole of government systems must be hosted in a Certified Strategic (previously referred to as sovereign) or Certified Assured Data Centre.

As part of risk management, DTA will support agencies to specify consistent minimum levels of certification for certain systems and data sets, for example, requiring that any reusable platform must be hosted in a Certified Strategic Data Centre.

Certification Overview

Certification under the Framework provides assurance to agencies that certified hosting providers meet defined security and risk management standards and have mitigation measures in place that support the outcomes set out in the Hosting Strategy.

A higher level of certification under this Framework does not guarantee an award of contracts, nor does a lower level of certification preclude the award of contracts.

Certification Levels

Uncertified Provider

Providers who do not seek or obtain certification under this Framework will be considered 'Uncertified'. Agencies may, however, use such uncertified providers for specific settings if their risk assessment determines it is appropriate for them to do so.

A breach of certification may result in a hosting provider becoming an uncertified provider and triggering remediation provisions under this Framework, as well as the provisions of the PSPF, FIRB or, once legislated, the Security Legislation Amendment (Critical Infrastructure) Bill 2020 (CI/SoNS).

Certified Assured Hosting Provider

This certification level provides for a stringent initial assessment and the inclusion of clauses in contracts to safeguard against a significant change in ownership, control or the operation of the provider which would increase the risk profile of the provider's Commonwealth tenants. These clauses also seek to minimise the transition costs associated with exiting the data centre due to a breach of these contract clauses.

Any information made available by providers under the initial certification assessment or continuous disclosure provisions of the Framework will also be matched against evidence available from other government entities.

Certified Strategic Hosting Provider

This certification level builds upon the Assured Certification and offers agencies additional protection through confirmation/guarantees undertaken by the provider that there will be no significant change in strategic direction, operation or ownership of the provider which would adversely affect:

- the level of confidence the Australian public has in the Commonwealth
- the Commonwealth's interests, and
- the certainty of services delivered to tenants for the life of the current government contract/s.

The Strategic Certification level provides for a more comprehensive initial assessment and the inclusion of clauses in contracts to cover the full reasonable transition costs associated with exiting the data centre due to a breach of these contract clauses.

Additionally, Certified Strategic Hosting Providers will be required to demonstrate their ability to record, manage and mitigate supply chain risks by:

- adhering to a formal, standards-based risk management framework with supporting recording tools, such as matrices, allocation of roles and responsibilities, and the regular review of treatments to mitigate the risks;[1] and
- vetting of key personnel by an Australian Government Security Vetting Agency (AGSVA) approved vetting company consisting of police, identity and reference checks, and the right to work in Australia; and
- providing remote-in support from locations that do not pose a threat to the Commonwealth.

Once certified, providers must demonstrate their ongoing status by:

- ongoing reporting as required under the Data Centre Facilities Supplies Panel; and
- continuous proactive disclosure of any information or ‘Relevant Change’ that would have a material effect on the ownership, control or operation of the

[1] The review period will depend on the level of risk being addressed, i.e. high, medium or low, with increased frequency as the risk level increases.

provider's core capabilities and that would alter the risk profile of the Commonwealth tenants; and

- periodic review of the providers' implemented controls for mitigation of supply chain risks.

Any information made available by providers under the initial certification assessment or continuous disclosure provisions of the Framework will also be matched against evidence available from other government entities.

The table below summarises the differences between the different levels of certification:

	Certified Strategic	Certified Assured	Uncertified
Data Centre Facilities Supplies Panel on-going reporting	✓	✓	✓
Initial posture assessment	✓	✓	✗
Ownership, Control & Operations Safeguards	✓	✓	✗
Proactive disclosure requirements	✓[2]	✓	✗
Periodic reviews	✓[2]	✓	✗
Minimise transition out costs	✓	✓	✗
Ownership, Control and Operations Guarantees	✓	✗	✗
Cover reasonable transition out costs	✓	✗	✗
Standards-based risk management framework obligations	✓	✗	✗

[2] Enhanced requirements apply to Certified Strategic Hosting Providers.

Vetting of key personnel	✓	✗	✗
Remote-in support restrictions	✓	✗	✗
Supply chain requirements	✓	✗	✗
PSPF	✓	✓	✓
FIRB	✓	✓	✓
Security Legislation Amendment (Critical Infrastructure) Bill 2020 (CI/SoNS)	✓	✓	✓

Table 4 Comparison of certification levels

Gaining Certification

Each provider must determine the level of certification it will seek to be assessed against.

DTA will work with a cross-agency team to undertake the certification and verify the information provided by the providers seeking to undertake certification.

The process required to achieve certification for different levels of certification is outlined below.

Certified Assured Hosting Provider

Providers seeking to become Certified Assured Hosting Providers will be required to:

- pass a stringent initial assessment of their current structure, ownership and control;
- agree to include relevant safeguard clauses in all future contracts with Commonwealth agencies;
- seek approval before any ‘Relevant Change’; and

- sufficiently reimburse the Agency to minimise transition costs borne by the Commonwealth associated with exiting the data centre if required.

Topic	Control / Clause	Risk / Rationale
Visibility of ownership	Seek the Agency's approval before any 'Relevant Change' occurs.	Changing hosting arrangements mid-contract due to risks created by changes in ownership, access and control is not in the interests of Government or industry.
Minimise impact	Include any measures reasonably directed by the Agency to mitigate or reduce the impact of the 'Relevant Change'.	Mitigates the risk, expense and impact of undesirable changes in supply chain and data centre ownership, control and use.
Reimbursement	Reimburse the Agency its reasonable costs associated with exiting the data centre.	Mitigates the risk, expense and impact of undesirable changes in supply chain and data centre ownership, control and use.
Reimbursement	The Agency is required to put in place measures to mitigate the impact of the 'Relevant Change'.	Mitigates the risk, expense and impact of undesirable changes in supply chain and data centre ownership, control and use.

Table 5 Certified Assured Controls

Certified Strategic Hosting Provider

Providers seeking to become Certified Strategic Hosting Providers will be required to:

- pass a more comprehensive initial assessment of their current structure, ownership and control, key personnel and supply chain;
- agree to more stringent clauses guaranteeing stability of ownership, real estate and assets deemed core capabilities, and ensure that the DTA and the contracting agency remain fully informed of events that may lead to a 'Relevant Change';
- seek approval before any 'Relevant Change';
- agree to clauses to confirm the Provider's ability to mitigate supply chain risks, and agree to periodic reviews of supply chain risk mitigation; and
- reimburse the Agency to cover reasonable transition costs borne by the Commonwealth associated with exiting the data centre if required.

Topic	Control / Clause	Risk / Rationale
Continuity of ownership; **Influence over direction;** **Visibility of direction.**	No significant change in strategic direction or ownership of the provider.	Meets the strategy requirement for ownership and control conditions. Changing hosting arrangements mid-contract due to risks created by changes in ownership, access and control is not in the interests of Government or industry.
Control over land and real estate	There will not be a sale or disposal of land which houses the data centre facility or any transfer, assignment, disposal of any lease or real estate related to the data centre facilities.	Meets the strategy requirement for ownership and control conditions.
Standard of service continuity	No changes to the security measures and procedures.	Meets the strategy requirement for ownership and control conditions.
Timely disclosure	Disclose sufficient information required by the DTA and the relevant Agency to ensure that the DTA and the relevant Agency remain fully informed of events that may lead to a 'Relevant Change'.	Fully informed to mitigate against the risk of change.
Reimbursement	Reimburse the Agency its total reasonable costs associated with exiting the data centre.	Mitigates the risk, expense and impact of undesirable changes in supply chain and data centre ownership, control and use.
Evidence	Consent for certifying authority/DTA to obtain information from other government entities.	Safety net to verify provider input.

Table 6 Certified Strategic Ownership Controls

Topic	Control / clause	Risk / Rationale
Supply chain risk management plan	Contractor must submit the Risk Management Plan to the DTA and the Agency on the Contract Start Date or at such other time as reasonably required by the DTA or the Agency. The Risk Management Plan should, as a minimum, comply with risk management standards AS/NZS ISO 31000:2018 and AS/NZS ISO 28001:2007.	Definition and documentation of relevant risks.
Supply chain risk management plan detail	The Contractor's supply chain risk management plan and processes to identify, manage and report risks and to ensure business and supply chain continuity.	Evidence of maturity of processes, capability.
	Methods and methodology for risk identification, rating, monitoring and treatment.	Ideally standards-based for consistency and recognised approach.
	Requirements for developing and maintaining a risk register to record and review risks.	Evidence of risk recording, mitigation measures, review and responsibilities.
	Allocated roles and responsibilities, including who within the Contractor's organisation will be responsible for the management, treatment and reporting of the relevant risks.	Confirmation of roles within the organisation and associated responsibilities.
Supply chain risk management plan review	Review and test its Risk Management Plan and risk management policies and procedures throughout the Contract Period and report the results to the DTA.	Evidence of currency of risk / treatment documentation and monitoring of risk mitigation.
	Promptly make any amendments required by the DTA and the Agency and resubmit the revised Risk Management Plan to the DTA and the Agency.	Ensure quality and detail of content to risk management plan.
Vetting of key personnel	Vetting key personnel by an Australian Government Security Vetting Agency (AGSVA) approved vetting company.	Ensure the integrity of key supply chain personnel.
Remote support requirements	Providing support from secure locations that do not pose a security threat to the Commonwealth.	Minimise the risk of cyber-attack and data breach.

Table 7 Certified Strategic Supply Chain Risk Controls

Certification approvals at each level will be made by the DTA Deputy Chief Executive Officer (DCEO) or an authorised delegate.

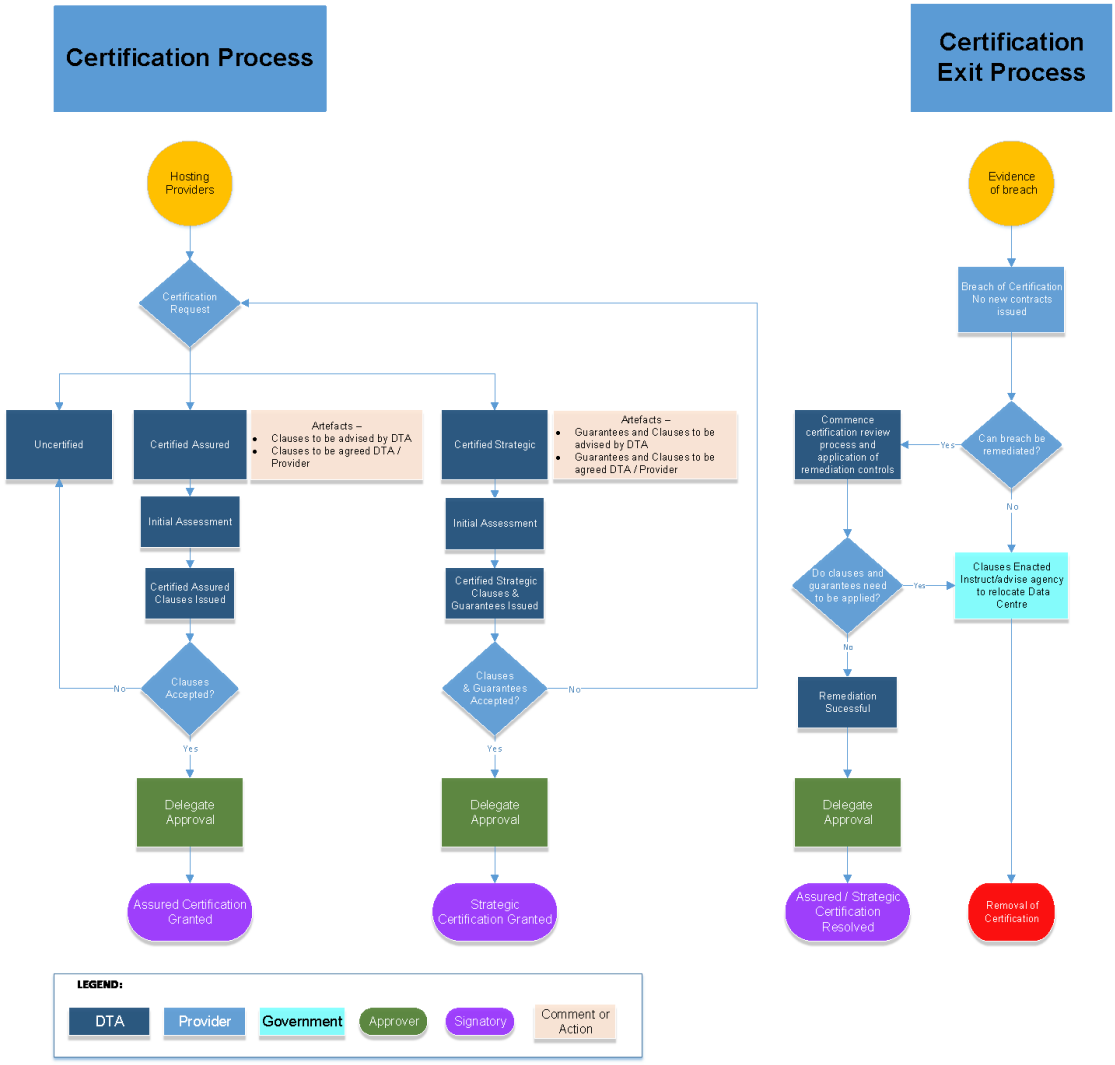

Figure 2 Certification Process Flow

Maintaining Certification

A key principle underpinning a provider's ability to maintain their certification is continuous disclosure of any relevant change.

In terms of the Certification Framework, a **'Relevant Change'** includes:

i. a change in the provider's Board or management team, the data centre security manager or other personnel, or subcontractors involved in the provision of the data centre facilities or services that has the potential to affect the Commonwealth, the Commonwealth's security interests, or the

delivery of the data centre services in accordance with the Head Agreement and Contract

ii. a significant change in strategic direction or ownership of the provider that has the potential to adversely affect the reputation of the Commonwealth, the Commonwealth's security interests, or the delivery of the data centre services in accordance with the Head Agreement and Contract

iii. a sale or disposal of land which houses the data centre facility or any transfer, assignment, disposal of any lease or real estate related to the data centre facilities that has the potential to adversely affect the reputation of the Commonwealth, the Commonwealth's security interests, or the delivery of the data centre services in accordance with the Head Agreement and Contract

iv. a change to the security measures and procedures, including the security measures and procedures at, or otherwise in relation to, the data centre facility that decreases the level of security at the data centre facility or poses a security threat to the Commonwealth or any data hosted within the data centre

v. any other event or circumstance relating to the security or operations of the data centre as set out in the Contract

Guidance Documents

For additional information related to the Framework, please refer to the below guidance documents:

- Whole-of-Government Hosting Strategy
- Australian Government Protective Security Policy Framework (PSPF)
- Information Security Manual (ISM)
- Public Governance, Performance and Accountability Act 2013 (PGPA Act)
- Department of Treasury – Foreign Investment Review Board (FIRB), Foreign Acquisitions and Takeovers Act 1975 (FATA Act), and Foreign Acquisitions and Takeovers Regulation 2015
- Commonwealth Procurement Rules, and
- The Department of Home Affairs – Protecting Critical Infrastructure and Systems of National Significance.

Glossary and Abbreviations

Term	Definition or Description
Agency	A Commonwealth entity within the meaning of the *PGPA Act 2013* and *PGPA Rules 2014*
CA	Certified Assured
CIO	Chief Information Officer
CS	Certified Strategic
DTA	Digital Transformation Agency
Home Affairs, DHA	Department of Home Affairs Of interest: • Protecting Critical Infrastructure and Systems of National Significance Consultation Paper • *Security of Critical Infrastructure Act 2018*
FIRB	Foreign Investment Review Board
Key Personnel	Supply chain personnel providing service to the data centre with an access pass to technical areas, and areas containing plant and equipment critical to the data centre's operation e.g., cleaners, security personnel, technicians, and maintenance personnel
Panel Two	Panel Two of the Data Centre Facilities Supplies Panel administered by the DTA
PSPF	The Protective Security Policy Framework managed by the Attorney General's Department (AGD)
Relevant Change	As defined within legal clauses in the Appendix, clause d
WofG	Whole-of-Government Sometimes WoAG for Whole of *Australian* Government

Appendix: Certification Clause Outlines

Outline clauses that apply to Certified Assured

Providers seeking to secure a Certified Assured status will be required to:

a. Acknowledge that a **'Relevant Change'** includes:

   i. a change in the provider's Board or management team, the data centre security manager or other personnel, or subcontractors involved in the provision of the data centre facilities that has the potential to affect the Commonwealth, the Commonwealth's security interests, or the delivery of the providers services in accordance with the Head Agreement and Contract.

   ii. a significant change in strategic direction or ownership of the provider that has the potential to adversely affect the reputation of the Commonwealth, the Commonwealth's security interests, or the delivery of the providers services in accordance with the Head Agreement and Contract.

   iii. a sale or disposal of land which houses the data centre facility or any transfer, assignment, disposal of any lease or real estate related to the data centre facilities that has the potential to adversely affect the reputation of the Commonwealth, the Commonwealth's security interests, or the delivery of the providers services in accordance with the Head Agreement and Contract.

   iv. a change to the security measures and procedures, including the security measures and procedures at, or otherwise in relation to, the data centre facility that decreases the level of security at the data centre facility or poses a security threat to the Commonwealth or any data hosted within the data centre.

   v. any other event or circumstance relating to the security or operations of the data centre as set out in the Contract

b. seek the Agency's approval before any ’Relevant Change’ occurs. Such approval may be given or withheld at the Agency's sole discretion and subject to conditions.

c. if requested, provide the Agency with information in relation to the ‘Relevant Change’.

d. cooperate with the Agency to assess and mitigate any adverse impacts of the ’Relevant Change’ on the Commonwealth.

e. implement any measures reasonably directed by the Agency to mitigate or lessen the risks or adverse impacts that may arise from the ’Relevant Change’.

f. reimburse the Agency its reasonable costs associated with exiting the data centre capped at an agreed percentage of the total contract value, if the provider fails to meet any of the above requirements.

g. without limiting paragraph e), where the Agency is required to put in place measures to mitigate the impact of the ’Relevant Change’, reimburse the Agency the reasonable costs incurred by the Agency capped at an agreed value to implement those measures.

h. acknowledge that the failure to comply with the above requirements may affect the provider's certification status.

i. agree to clauses that, in addition to the rights under the Head Agreement, give the Agency the right to immediately terminate the Contract and the DTA the right to terminate the Head Agreement if, in the Agency's or the DTA's reasonable assessment, the provider has failed to comply with the above requirements.

j. providers give express consent for certifying authority/DTA to obtain information from other government entities and for this information to be used for any purpose in connection with the provider’s certification.

Outline clauses that apply to Certified Strategic

Providers seeking to obtain Certified Strategic status will be required to:

a) Acknowledge that a **'Relevant Change'** includes:

i. a change in the provider's Board or management team, the data centre security manager or other personnel, or subcontractors involved in the provision of the data centre facilities or services that has the potential to affect the Commonwealth, the Commonwealth's security interests, or the delivery of the providers services in accordance with the Head Agreement and Contract.

ii. a significant change in strategic direction or ownership of the provider that has the potential to adversely affect the reputation of the Commonwealth, the Commonwealth's security interests, or the delivery of the providers services in accordance with the Head Agreement and Contract.

iii. a sale or disposal of land which houses the data centre facility or any transfer, assignment, disposal of any lease or real estate related to the data centre facilities that has the potential to adversely affect the reputation of the Commonwealth, the Commonwealth's security interests, or the delivery of the providers services in accordance with the Head Agreement and Contract.

iv. a change to the security measures and procedures, including the security measures and procedures at, or otherwise in relation to, the data centre facility that decreases the level of security at the data centre facility or poses a security threat to the Commonwealth or any data hosted within the data centre.

v. any other event or circumstance relating to the security or operations of the provider as set out in the Contract.

b) without limiting any disclosure requirements under the Head Agreement, continuously disclose sufficient information required by the DTA and the relevant Agency to ensure that the DTA and the relevant Agency remains fully informed of events that may lead to a 'Relevant Change'.

c) seek the Agency's approval before any ’Relevant Change’ occurs. Such approval may be given or withheld at the Agency's sole discretion and subject to conditions.

d) confirm/guarantee that there will be no Relevant Change that has the potential to adversely affect the reputation of the Commonwealth, the Commonwealth's security interests, or the delivery of the providers services in accordance with the Head Agreement and Contract.

e) reimburse the Agency its total reasonable costs associated with exiting the data centre, as well as any reasonable additional costs incurred by the Agency as a result of the provider's failure to meet the above requirements.

f) acknowledge that the failure to comply with the above requirements may affect the provider's certification status.

g) agree to clauses that, in addition to the rights under the Head Agreement, give the Agency the right to immediately terminate the Contract and the DTA the right to terminate the Head Agreement, if, in the Agency's or the DTA's reasonable assessment, the provider has failed to comply with the above requirements.

h) providers give express consent for certifying authority/DTA to obtain information from other government entities and for this information to be used for any purpose in connection with the provider’s certification.

Additionally, the provider's (and where applicable, ultimate parent company's) directors and relevant officers/Board members will be required to provide a declaration that they are aware of the above requirements and that they will use their best endeavours to ensure that the events and circumstances specified as a Relevant Change in paragraph a) above do not occur.