Government Chief Digital Office

Marketplace Information Security Tiering Standard For Infrastructure Services Telecommunications Services Managed Security Services Channels

Issued by AoGSD Security Team

Internal Affairs
Te Tari Taiwhenua

New Zealand Government

Document Control

Document Name	Marketplace Information Security Tiering Standard
Author	All of Government Services Delivery (AoGSD)
Version	V1.0 17 February 2026
Document Number	GCDO.MKP.Standard.2025_175

Confidentiality

Revision History

Version	Date	Author	Description of changes
1.0	17/2/2026	GCDO Security	Initial release

Table of Contents

Marketplace Security Assurance Tiering Definitions

1. Background

The following Information Security Assurance Tiering definitions have been developed to support the transition for Infrastructure as a Service (IaaS) and Telecommunications as a Service (TaaS) commercial constructs into the Marketplace.

This Information Security Assurance Tiering definitions currently apply to the following channels (I/T/MS):

Information Security Assurance Tiering definitions:

- Infrastructure Services
- Telecommunications Services
- Managed Security Services

2. Security Assurance Tiering Descriptions

The table below defines each of the Security Assurance and Certification Tiers. Tiers correspond to the level of security assurance requirements against which organisations and their Services will be assessed, during onboarding and/or thereafter, and therefore the level of centralised security assurance DIA is able to give purchasing agencies.

Table 1: Security Assurance Tiering Descriptions

Tier	Description
Tier 4 – Professional Services	Tier 4 requires providers to answer onboarding questions to DIA's satisfaction and provide evidence they have the appropriate qualified and trained staff to perform the services for which they apply for Marketplace services listings provider.
Tier 3 – Baseline	Tier 3 requires providers to answer baseline questions and the 'provider questions' in the Cloud Risk Discovery Tool[1] questions to DIA's satisfaction.
Tier 2 – Provider Security Assurance	Tier 2 requires an appropriate level of security assurance to support consuming agencies Certification and Accreditation requirements. But at a level that is lower than centralised Tier 1 Information Security Certification. **Tier 2 Endorsement** is required prior to agencies consuming services and is achieved through providers providing: As part of a provider being approved onto the Marketplace, as part of onboarding they are required to provide: a. an independent audit of GCDO defined **Organisational Controls**, at a minimum of the Cyber Security Capability Maturity Model (CS-CMM) CS-CMM2[2]. The report provided to GCDO will be assessed for Tier 2 Endorsement, as per GCDO's Continuous Security Certification Control Validation Plan - Organisation Controls. Plus, for **Service Controls**:

[1] Cloud Service Provider Risk Assessment Questionnaire for GCDO Compliance – The provider subset of the Cloud Risk Discovery Tool questionnaire.

[2] NCSC Cyber Security Capability Maturity Model (CS-CMM) Minimum Cyber Security Standards. The CS-CMM capability maturity model is used to assess a providers security capability. To confirm they are appropriate for the management of NZ government ICT and protection of NZ government and NZ citizen information.

Tier	Description
	a. a completed self-assessment of each service. Meeting a minimum of CS-CMM2 of GCDO's Continuous Security Certification Control Validation Plan - Service Controls; or b. SOC II Type 2 report; and c. Independent Technical Testing reports[3].
Tier 1 – Service Information Security Certification	Tier 1 equates to Information Security Certification. Once there are two agencies consuming the provider Marketplace service the GCDO Continuous Security Certification[4]process is to commence. Providers are to engage with GCDO within one month of the second agency consuming the service. The Continuous Security Certification (CSC) process is to start within three months of the second agency consuming the service or a timeframe agreed with the GCDO Security team Services that require Tier 1 certification need to first meet Tier 2 security assurance requirements. An independent audit is to be performed against the GCDO Continuous Security Certification - Controls Validation Plan. This includes both Organisation and Service controls. The first CSC assessment is to confirm a provider meets CS-CMM3 for Physical, Personnel, Multi-Factor Authentication and Least Privilege for both Organisation and Service control areas. CS-CMM2 must be achieved for all other Organisation and Service control areas. For certification to be achieved the second CSC assessment (first Maintenance review) all control areas for Organisation and Service must be at CS-CMM3. We support the reuse of Third Party independent audits such as ISO (for organisation controls) and SOC II Type 2 (for service controls)[5]. Tier 1 Service Information Security Certification is made up of two parts: • Tier 1 – Organisation Controls Security Certificate Tier 1 – Service Security Certificate

[3] This may include the use of Third Party cloud services Penetration Testing reports.

[4] Marketplace Information Security Assurance and Certification Process is available on GETs and the Marketplace dashboard.

[5] GCDO control areas has been mapped to PSR/NZISM/PCIDSS/NIST 800-53/ISO 27001/SOC 2 Type II. To support the reuse of Third Party audit reports, clear traceability of controls to services needs to be clearly articulated by providers and their auditors.

Tier	Description
Tier 1 – Data Centre Certification	Tier 1 Data Centre Certification is an assessment of the Facility and specified Data Halls. It is required if the provider is delivering cloud hosted government services. A provider may request certification of their Data Hall if the Data Centre Facility is certified. As per GCDO's Data Centre Controls – Control Validation Plan. Providers who have achieved Public Cloud Data Centre Certification will be required to audit any delta controls. A gap analysis between both control sets is being done by GCDO. • Tier 1 – Organisation Controls Security Certificate (this is required if not achieved via a Service's certification). • Tier 1 –Data Centre Security Certificate[6].

3. Tiering related to Service Constructs

The table below defines the default Security Assurance Tiering that will apply for services to be listed in the Infrastructure Services Channel, Telecommunications Services Channel, and Managed Security Services Channel of the Marketplace, dependent on the mix of responsibilities of the parties involved in delivering the Service:

a. Where a provider is responsible for managing the service, it will require Tier 1 Certification.

b. Where the agency is responsible for managing the service, it will require Tier 2 Security Assurance to be performed.

c. There is opportunity for exceptions if providers can present evidence that staff do not have access to Agency data. Or the ability to grant access Lead Agency will assess if the service can be Tier 2.

d. The delivery of managed services is reliant on the provider. Security assurance is required to ensure the delivery cannot be undermined. The criticality of the service and impact on the NZ government will be considered should a provider request a service is assessed at Tier 2, rather than Tier 1 as defined below.

Table 2: Service Construct Descriptions

Managed Support (agency-specific hardware or software configuration/management)	Software (licensing ownership – who pays the subscription to the Cloud or COTS software vendor)	Infrastructure/Hardware (includes operating system or built in software) that runs this service and stores the agency data.	Tier
Security Tiering – Common Service Scenarios			
Marketplace Provider	Marketplace Provider	Marketplace Provider	1

[6] Any duplicate controls between Organisation and Data Centre CVP only need to be validated through the Organsiation review. GCDO will remove any duplicated controls from the Data Centre CVP.

Managed Support (agency-specific hardware or software configuration/management)	Software (licensing ownership – who pays the subscription to the Cloud or COTS software vendor)	Infrastructure/Hardware (includes operating system or built in software) that runs this service and stores the agency data.	Tier
Example Services: • Local Area Network service – equipment owned, operated and fully managed by Marketplace Provider. • Wide Area Network service – equipment owned, operated and fully managed by Marketplace Provider plus Third Party providers of service, e.g. Chorus. • Non-public cloud Virtual Compute services (infrastructure owned and operated by Marketplace Provider).			
Agency	Marketplace Provider	Marketplace Provider	2
Example Services: • Firewall with agency management – equipment and licensing owned by Marketplace Provider, sold as a monthly service with break/fix, however agency manages the infrastructure, configuration, backup, patching etc. Marketplace Provider has no access to agency configuration or data. • Visitor Management – service hosted and break/fix support provided by Marketplace Provider, agency undertakes all administration. Marketplace Provider has no access to agency configuration or data.			
Agency	Agency	Marketplace Provider	2
Example Services: • Meeting Room – in-room video conferencing equipment owned and supported by Marketplace Provider. Agency owns software subscription directly from a Third Party Cloud Service Provider (not part of this service in Marketplace) and configures software (e.g. Microsoft Teams).			
Marketplace Provider	Agency	Agency	1
Example Services: • Data Networking Managed Services – an agency owns their own equipment and outsources the management to a Marketplace Provider. • Infrastructure Managed Services – an agency owns their own equipment and outsources the management to a Marketplace Provider • Note: Marketplace certification scope would be limited to the Marketplace Provider's management service scope only, in this scenario the Agency would be responsible for certifying the underlying software and hardware.			
Marketplace Provider[7]	Agency	Third Party Cloud Service Provider[8]	1

[7] DIA Contracted Marketplace provider.

[8] Third Party cloud supplier to either the Marketplace provider or the Agency.

Managed Support (agency-specific hardware or software configuration/management)	Software (licensing ownership – who pays the subscription to the Cloud or COTS software vendor)	Infrastructure/Hardware (includes operating system or built in software) that runs this service and stores the agency data.	Tier
Example Services: • UC Managed Services – Marketplace Provider is managing an agency's solution for Unified Communications that they have procured directly from a Third Party Cloud Service Provider (e.g. MS Teams). • Note: Marketplace certification scope would be limited to the Marketplace Provider's management service scope only, in this scenario the agency would be responsible for certifying the underlying cloud service.			
Marketplace Provider	Marketplace Provider	Third Party Cloud Service Provider	1
Example Services: • Cloud Access Security Broker – cloud service resold by Marketplace Provider who is also managing the cloud service on behalf of the agency. • Public Cloud Virtual Compute services resold by Marketplace Provider.			
Agency	Marketplace Provider	Third Party Cloud Service Provider	3
Example Services: • Contact Centre – cloud service resold by Marketplace Provider, however the agency manages their own configuration. The Marketplace Provider has no access to agency data. • Or if the Marketplace Provider is a licence reseller only.			
Agency	Agency	Third Party Cloud Service Provider	3
Example Services: • Any pure cloud service purchased by an agency.			
Security Tiering – Hybrid Service Scenarios			
Marketplace Provider	Marketplace Provider	Third Party Cloud Service Provider Marketplace Provider	1
Example Services: • Fully managed service by Marketplace Provider that incorporates a resold Cloud-based contact centre with additional Marketplace Provider-provided add-ons such as network-based intelligent routing.			
Agency	Marketplace Provider	Third Party Cloud Service Provider Marketplace Provider	2
Example Services: • Agency-managed service where a Marketplace Provider offers a resold Cloud-based contact centre with additional Marketplace Provider-provided add-ons such as network-based intelligent routing. Marketplace Provider does not have access to agency data.			
Security Tiering – Specific Services			

Managed Support (agency-specific hardware or software configuration/management)	Software (licensing ownership – who pays the subscription to the Cloud or COTS software vendor)	Infrastructure/Hardware (includes operating system or built in software) that runs this service and stores the agency data.	Tier
Data Centres owned and operated by the Marketplace Provider. Data Centres will follow the Traditional GCDO Data Centre certification process and the Organisation component of the Continuous Security Certification process. Public Cloud Data Centre Certifications will be reused for Marketplace. Gap analyses between the audit scope for Public Cloud Data Centre Certification and Marketplace Data Centre certification is being determined and will be made available to providers on request.			1
PSTN Access			2
Mobile Network			2

4. Onboarding Security Assurance

Standard onboarding to ICT Common Capability contracts provides a primary procurement review as part of initial assessment of a single set of criteria and controls. These criteria and controls are based on the Protective Security Requirements (PSR), New Zealand Information Security Manual (NZISM) and industry standards.

The following criteria and artefacts will be reviewed and assessed by GCDO's Security team for the (IT/MS) channels:

Table 3: Onboarding Security Assurance

Tier	Onboarding Security Assurance	2+ Agencies – Information Security Certification
Tier 4 – Professional Services	1. GCDO's review of provider responses to onboarding requirements.	Not Applicable The number of agencies consuming services does not trigger certification.
Tier 3 – Baseline Review	1. GCDO's review of provider responses to onboarding requirements. 2. GCDO's review of provider Cloud Terms Agreements – Cloud Service Provider Risk Questionnaire for GCDO Compliance[9].	Not Applicable The number of agencies consuming services does not trigger certification.

[9] Pae Hokohoko | Marketplace — Apply to be a Provider

Tier	Onboarding Security Assurance	2+ Agencies – Information Security Certification
Tier 2 – Provider Security Assurance	1. GCDO's analysis of provider responses to onboarding requirements. 2. GCDO's analysis of Cloud Terms Agreements – Cloud Service Provider Risk Questionnaire for GCDO Compliance. **Tier 2 Endorsement** 3. GCDO Tier 2 Endorsement[10] of Organisation Controls (initial independent audit – to CS-CMM2 (moving to CS-CMM3 for Tier 1 Information Security Certification[11]). 4. GCDO Tier 2 Endorsement of either provider self-assessment of Service/s Controls or SOC2 and independent Technical Test/s.	As soon as two agencies are consuming the service, Tier 1 certification is required to start within three months from the date of the second agency's consumption (or as agreed with GCDO Security team).
Tier 1 – Information Security Certification	Providers are not onboarded at Tier 1.	

5. Security Assurance Lifecycle Schedule

Once a provider has been successfully onboarded to the IaaS/TaaS and Managed Security Channels in the Marketplace, the annual security assurance lifecycle will begin. Annual security assurance is also referred to as Maintenance reviews.as suppliers are expected to:

- Confirmed as achieving CMM3 across all control areas during the first Maintenance review; and
- Maintain control areas at CMM3 annually for Organisation and Service(s).

Table 4: Security Assurance Lifecycle Schedule

	Certification and Renewal	Security Assurance Yearly Maintenance Cycle[12]
Organisation Certification	Initially and then every 3 years	Continuous Security Certification (CS-CMM3)
Data Centre Certification	Initially and then every 3 years	Annual Audit Assurance

[10] As Organisational Controls are used across all services and to reduce effort certification is initiated here. Providers should be assessed at CS-CMM3, and needs to happen within 12 months. This will need to be confirmed during the second Continuous Security Certification review, if not during the first assessment.

[11] Evidence from ISO or SOC2 can be used as evidence.

[12] This is being included in the documentation being developed by Lead Agency for Continuous Security Certification.

Tier 1 Information Security Certification	Initially and then every 3 years	Continuous Security Certification (CS-CMM3)
Tier 2	Initially and then every 3 years	Tier 2 Endorsement (CS-CMM2)
Tier 3	Certification is not required. Supporting Marketplace documentation needs to be updated when changes that may impact on the security aspects of the service.	Certification is not required. Supporting Marketplace documentation needs to be updated when changes that may impact on the security aspects of the service.
Tier 4	Not Applicable	Not Applicable