

# Guide: Infrastructure as a Service

Access to public cloud services  
- agency guidance

# Document purpose

This document provides guidance to New Zealand government agencies about the Microsoft and Amazon Web Services (AWS) public cloud services that can now be accessed through the Infrastructure as a Service (IaaS) agreement. It will be updated as public cloud services evolve and as the Department of Internal Affairs (DIA) issues additional supporting documentation, such as risk assessments and security certifications.

## Contents

<b>Introduction .....</b>	<b>3</b>
Key contact .....	3
<b>Background .....</b>	<b>4</b>
IaaS public cloud services .....	4
Contractual arrangements .....	4
<b>Description of services available .....</b>	<b>5</b>
<b>How do agencies consume these services? .....</b>	<b>6</b>
<b>Glossary of abbreviations and terms .....</b>	<b>8</b>
<b>Appendices .....</b>	<b>9</b>
Appendix A: Options to consume Microsoft's Azure services .....	9
Appendix B: Options to consume Amazon Web Services (AWS) .....	10
Appendix C: High level flow to illustrate public cloud access via IaaS .....	11
Appendix D: IaaS Service Characteristics .....	12

# Introduction

The Government IaaS agreement enables agencies to meet their medium and long-term goals for government ICT infrastructure services through:

- access to cheaper services, through a consumption model combined with discounts available through aggregated demand
- rationalisation of government's ICT assets, providing delivery of lower overall cost to government
- the provision of a foundation for moving into a cloud computing model, allowing access to more cost efficiencies, productivity and service benefits.

The ability for agencies to consume Amazon Web Services and Microsoft's public cloud services through the IaaS agreement enables agencies to:

- obtain reduced pricing from leveraging aggregated demand for these services;
- integrated billing; and,
- a single view across on-shore and off-shore hosted infrastructures services.

The scope of the public cloud services available via the IaaS service catalogues of public cloud services is **utility compute and storage**. This guidance defines these terms in relation to the definitions used in the Amazon Web Services and Microsoft service catalogues.

There is no requirement to undergo a full procurement process if agencies consume these services through the IaaS agreement. Agencies are, however, recommended to use a secondary procurement process.

## Key contact

For further information, please contact:

The Department of Internal Affairs

**Sophary Dim**

All-of-Government ICT Capability Manager

+64 4 463 1396

+64 21 906 087

[sophary.dim@dia.govt.nz](mailto:sophary.dim@dia.govt.nz)

## Background

In October 2011, the Department of Internal Affairs (DIA) entered into a Syndicated Agreement with three panel suppliers – Datacom (NZ) Ltd, Revera Ltd and IBM New Zealand Ltd – for the provision of Infrastructure as a Service (IaaS) services.

IaaS is a managed and hosted infrastructure solution that contains four core services: data centre services, utility compute, storage, and back-up services to government agencies. In late 2013, the IaaS Syndicated Agreements were amended to Common Capability ICT Agreements.

The aim of IaaS is to enable government agencies to meet the medium and long-term goals for government ICT services through:

- access to cheaper services, through a consumption model combined with discounts available through aggregated demand;
- rationalisation of government's ICT assets, providing delivery of lower overall cost to government; and
- the provision of a foundation for moving into a cloud computing model, allowing access to more cost efficiencies, productivity and service benefits.

Public cloud services have become a mainstream technology choice for public and private sector organisations globally. The demand for public cloud services is growing among New Zealand public sector agencies. In response, the Government Chief Information Officer (GCIO) has considered how to enable agencies to consume public cloud compute and storage services through the IaaS common capability agreement.

Working within the constraints of the IaaS scope as defined in the original RFP and the Cabinet mandate for agencies to use IaaS, DIA has encouraged IaaS suppliers to resell public cloud compute and storage services to agencies through the IaaS agreement. Datacom and Revera have decided to resell Amazon Web Services (AWS) and Microsoft Azure (Azure) services.

## IaaS public cloud services

Datacom and Revera provide public cloud compute and storage services through their established reseller partnering agreements. Currently, IBM is not in a position to provide public cloud services. DIA will continue to work with IBM to enable these services, which are expected to be available in the future.

The expected agency use cases for IaaS public cloud services include: test and development, long-term archival and backup, public-facing websites, cloud native and applications. The value of consuming IaaS public cloud services through an IaaS supplier is integrated billing, reduced pricing from demand aggregation, and single management interface for all infrastructure services.

## Contractual arrangements

A description of public cloud services, including relevant terms and conditions, are detailed in *Section 8 (Resale of Third Party Public Cloud Services) of Datacom and Revera's IaaS service catalogues*. These service catalogues are updated when required. Consuming agencies will be notified of any changes made to these catalogues.

The commercial model allows the public cloud provider's contractual terms, conditions, and service levels to flow through to consuming agencies. This means these services **will not** be subject to the standard IaaS contractual terms and conditions and service levels.

## Description of services available

The scope of services available via the IaaS service catalogues of public cloud services has been defined as **utility compute and storage**. The description of these services is based on the definitions used by Amazon Web Services and Microsoft Azure service catalogues.

For clarity and simplicity, in-scope services are categorised as towers of Core Services and Supporting Services. Out of scope services are also specified for avoidance of doubt. A *Core* tower means that all of the services within that tower are within the scope of the IaaS RFP.

The categorisation of Azure and AWS's service catalogues is shown in the table below.

Type	Amazon	Microsoft
	<b>Compute</b>	<b>Compute</b>
Core	Storage and content delivery	Data and Storage
Core	Database	Media and CDN
Supporting	Networking	Networking
Supporting	Management tools	Management
Supporting	Security and identity	Identity and access management
Supporting	Application services	Hybrid integration
Out of scope	Analytics	Analytics
Out of scope	Enterprise Applications	n/a
Out of scope	Mobile services	Web and Mobile
Out of scope	Internet of things	Internet of things
Out of scope	Developer tools	Developer services

A *Core Services* tower includes database services (which are defined as databases that are ***neither configured, customised or are not managed*** on an on-going basis).

A *Supporting* tower means that all of the services within that tower are either necessary in order to consume one or more services within a *Core* tower or are complementary to one or more individual services within a *Core* tower. Services within a *Supporting* tower would not normally be consumed as a standalone service (e.g. AWS Direct Connect or MS Azure ExpressRoute). These towers are also considered in-scope and can be consumed through the IaaS agreements.

An *Out of scope* tower means that all of the services within that tower are out of scope of the IaaS RFP (e.g. Azure Analytics, AWS Enterprise Applications, AWS Internet of Things). Agencies may not use the IaaS contract when consuming any of the services from an 'out of scope' tower.

The mapping of 'towers' between the two services catalogues is largely one-to-one with the exception of storage, database, and content delivery, which are bundled slightly differently across the two 'towers' by Microsoft and Amazon. For the purposes of categorisation this difference is not material as storage, database, and content delivery all belong to 'core' towers.

It is recognised that the public cloud provider service catalogues are dynamic and DIA, in collaboration with the service providers, reserves the right to re-categorise services when required.

The IaaS Service Providers can also provide professional services under the IaaS agreements to assist with on-boarding, design, configuration and support of public cloud services.

Agencies can also use the ITMS agreement to consume the Supporting Services.

# How do agencies consume these services?

## Procuring service outside of IaaS

There is no restriction on government agencies using public cloud services that are outside the scope of the IaaS contract (compute and storage) as long as the services are not procured under the IaaS contract. Out of scope services can be procured using a separate agreement noting that agencies will have to comply with the Government Rules of Sourcing and also the GCIO mandated requirements and constraints that relate to the use of public cloud services.

**Note:** because this is a commercial re-sale model, public cloud provider's contractual terms and conditions and service levels will flow through to consuming agencies, and will **not** be subject to the standard IaaS contractual terms and conditions and service levels.

## Procuring IaaS public cloud services

Agencies who consider public cloud utility compute and storage services via the IaaS contract are recommended to use the Secondary Procurement Process in the same way as consuming onshore IaaS from Datacom, Revera and IBM, and do not need to undergo a procurement process.

Agencies will also need to be aware of their requirement to comply with the **Government Rules of Sourcing** to procure services outside of IaaS scope, such as Platform as a Service (PaaS) services.

The current IaaS standard contractual documentation –the Memorandum of Understanding (MoU) and the Participating Agency Agreement (PAA) – will apply, as does the application of the IaaS lead agency fee on consumption of operational services for onshore IaaS and public cloud utility compute and storage (including supporting services if consumed via IaaS PAA) services.

## Lead agency fees

The IaaS lead agency fee is currently 2.5% of monthly spend on operational services (onshore) and public cloud utility compute and storage services (and supporting services if they are consumed via the IaaS agreement). (Please note: the IaaS lead agency fee is under review and may be altered in the near future.)

## IaaS mandate

Agencies subject to the GCIO mandate to use IaaS can only procure public cloud infrastructure through the IaaS agreement as set out in this guidance.

## Cabinet policy on cloud computing

Agencies are able to use public cloud services to process and store data classified **RESTRICTED and Below**, noting that the agency must be aware of the requirements and constraints that relate to the use of cloud services:

(<https://www.ict.govt.nz/guidance-and-resources/information-management/requirements-for-cloud-computing>).

## Hosting locations

Currently the IaaS service providers are only reselling public cloud compute and storage services hosted in Australia. However, they will consider services hosted in other regions if agency demand warrants it.

## Security Certification

A generic IaaS public cloud risk assessment and security certificates for Amazon and Microsoft services are in development and will be made available to agencies once completed.

Agencies will need to accept the risks as identified in the generic cloud risk assessment (when available) and/or undertake their own risk to meet their specific public cloud use case by factoring in the technical and business contexts together with their specific requirements around personally identifiable Information (PII).

## Connectivity

There is no standardised connection model. An agency may choose to connect through their IaaS service provider's data centre by purchasing an optional connection offering from them (from the IaaS service catalogue), from the cloud provider (e.g. Microsoft Azure ExpressRoute or AWS Direct Connect), or from any third party. Agencies need to determine the 'characteristics' of the connectivity services they purchase, e.g. capacity and redundancy options.

# Glossary of abbreviations and terms

Term	Meaning
<b>AWS</b>	Is a subsidiary of Amazon.com, which offers a suite of cloud computing services that make up an on-demand computing platform.
<b>ICT Common Capability Services</b>	Refers to common capability contracts used in the procurement of information, communication and technology (ICT) services for use across government. These contracts are developed under the oversight of the Government Chief Information Officer (GCIO) at the Department of Internal Affairs (DIA) as the Functional Leader for Government ICT.
<b>Lead Agency</b>	An agency authorised to procure and manage ICT Common Capability Services. In most scenarios, the Lead Agency will be DIA.
<b>Participating Agency</b>	The Participating Agency is an agency that intends to use an ICT Common Capability Service (an Eligible Agency) or that has already subscribed to an ICT Common Capability contract (a Participating Party). In this process the Participating Agency is responsible for the certification of the Participating Agency's responsibilities and controls, and the subsequent accreditation of the service for use in that agency.
<b>Public Cloud services</b>	A cloud is called a "public cloud" when the services are rendered over a network that is open for public use.
<b>Microsoft Azure</b>	A cloud computing platform and infrastructure created by Microsoft for building, deploying, and managing applications and services through a global network of Microsoft-managed data centres.

## Related Documents

<b>Revera Service IaaS Catalogue</b>	Describes Revera's IaaS offering to government.
<b>Datacom Service IaaS Catalogue</b>	Describes Datacom's IaaS offering to government.

# Appendices

## Appendix A: Options to consume Microsoft's Azure services

Agencies have two options in how they can consume Microsoft Azure services.

### **Option 1: through G2015 via a Licensing Solutions Partner (LSP) using the Enterprise Agreement**

- (a) This option allows the agency to leverage pricing and terms and condition negotiated by DIA on behalf of government.
- (b) Agencies own and manage the Azure licences with the licences purchased through an LSP. This means that agencies will need to ensure they have adequate Azure services support – either resourced internally or outsourced to a supplier.
- (c) Agencies must provide access to Azure EA portal for the IaaS service provider to administer the provision of services. The IaaS service provider should be nominated as the partner of record.
- (d) It is recommended that agencies work with their LSP to understand fully their Microsoft licence ownership and therefore, what opportunities and/or leverages can be made using the existing licences to support the consumption of Azure.
- (e) The IaaS supplier will not bill agencies direct for services consumed. Billing will come from the LSP.
- (f) The IaaS Lead Agency fee will apply.

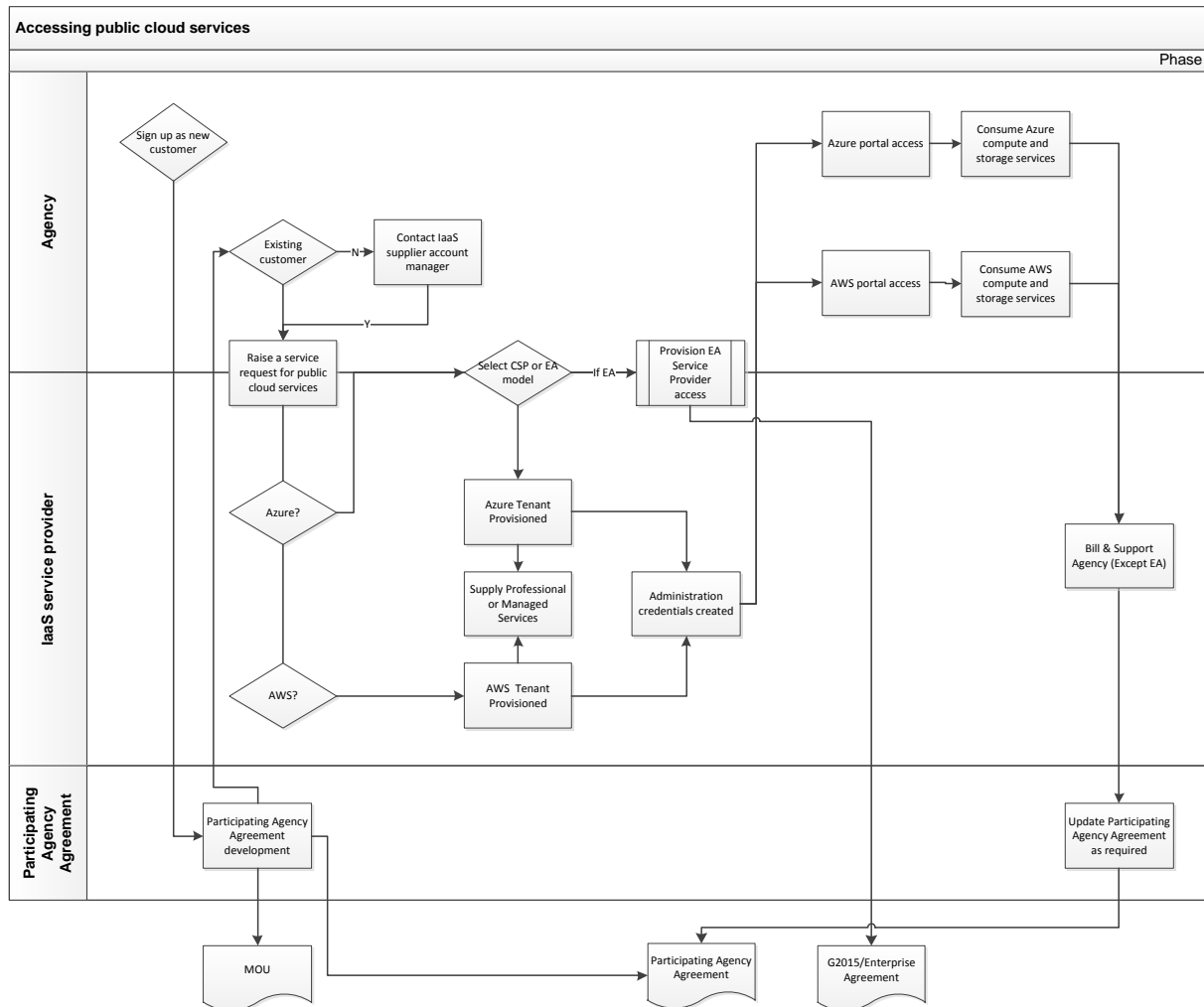
### **Option 2: using a Cloud Solution Provider (CSP)**

- (a) This is where the IaaS supplier contracts with Microsoft to offer public cloud services through Microsoft's CSP programme. As a CSP, the IaaS supplier will provide end-to-end services (e.g. account management and provisioning) and support (e.g. technical) services to the agencies wanting to consume Azure cloud services. As participant of the CSP program, Microsoft provides the ability for the IaaS supplier to create support requests with Microsoft when an issue arises that cannot be resolved without assistance from Microsoft. The CSP support benefit covers Microsoft Azure, Microsoft Dynamics CRM Online, Microsoft Intune, Enterprise Mobility Suite (EMS) and Microsoft Office 365.
- (b) As a CSP, the IaaS supplier is given delegated administration rights that enable them to effectively provide technical support to agencies. However, agencies have the option to remove a CSP's administration rights ability and manage it themselves. Note: this will not change the commercial relationship that a CSP transacting partner may have with an agency, but rather, it removes the ability for the IaaS supplier to administer the service on behalf of the agency. The IaaS supplier will still be responsible for providing support for the customer and adhere to any other terms of the Cloud Reseller Agreement.
- (c) The IaaS supplier will bill agencies direct for services consumed. This may include services consumed from Revera and Datacom's onshore IaaS services.
- (d) The IaaS Lead Agency fee will apply.

## Appendix B: Options to consume Amazon Web Services (AWS)

- (a) The IaaS supplier contracts with Amazon to offer public cloud services through Amazon reseller programme. As a reseller, the IaaS supplier will provide end-to-end services (e.g. account management and provisioning) and support (e.g. technical) services to the agencies wanting to consume AWS cloud services. As participant of the reseller program, Amazon provides the ability for Revera or Datacom to create support requests with Amazon when an issue arises that cannot be resolved without assistance from Amazon.
- (b) As an AWS reseller, the IaaS supplier is given delegated administration rights that enable them to effectively provide technical support to agencies under the terms of the Cloud Reseller Agreement.
- (c) The IaaS supplier will bill agencies direct for services consumed. This may include services consumed from the IaaS supplier's onshore IaaS services.
- (d) The IaaS Lead Agency fee will apply.

## Appendix C: High level flow to illustrate public cloud access via IaaS



## Appendix D: IaaS Service Characteristics

### Service Characteristics

Service Characteristic	Onshore IaaS	IaaS Public Cloud
Hosting	Onshore	Offshore (currently Australia)
DIA Certification	Yes	Under development
Security Classification	RESTRICTED AND BELOW	RESTRICTED AND BELOW (refer to Security Guidance from the cloud programme)
Service Management	Manned help desk and self-service	Limited / self service
Latency (dependant on connection option)	Minimal as hosted and accessed locally	Variable and higher than for onshore hosting
Service levels	Yes. As defined in the IaaS contract	Subject to change by third party cloud service provider
Service level credits	Yes. As defined in the IaaS contract and payable by service provider	As prescribed by the third party cloud service provider and subject to change by the third party cloud service provider
Supplier liability	As prescribed in the IaaS contract	As per Terms and Conditions from public cloud services provider.
Continuity of services	Requires Lead Agency approval to remove or amend services	No commitment to maintain continuity of current services
Pricing	Pricing is fixed with set volume price reductions	Variable pricing which is also subject to fluctuating exchange rate changes.