Te Tari Taiwhenua
Internal Affairs

45 Pipitea St
PO Box 805
Wellington 6140
Phone +64 4 495 7200
Fax +64 4 495 7222
Website dia.govt.nz

24 July 2024

Dave Watson
fyi-request-26791-64dcd9f1@requests.fyi.org.nz

Tēnā koe Dave,

Official Information Act 1982 request, reference OIA2324-0969

Thank you for your email of 14 May 2024 to Te Tari Taiwhenua | Department of Internal Affairs requesting the following under the Official Information Act 1982 (the Act):

> *I wish to better understand NZ Government use of cloud services and the uptake of such services through GCDO negotiated agreements.*
>
> *Please provide any "cloud plans" that were shared with the GCDO in the past 3 years. Agencies are required to have such plans for cloud adoption per digital.govt.nz*
>
> *Please provide any security, risk or privacy assessments of any NZ or international cloud service providers that DIA or relevant government organisations have undertaken (directly or indirectly through vendors) in the past 3 years including any reports into the integrity or suitability of these providers, detailing any concerns wrt. security, risk or privacy of NZ government use of these services. This should include all correspondence with these cloud service providers relating to assessments of audits of their services and mitigation of any related risks or issues relating to the providers service.*
>
> *Can GCDO provide any insight into the success or failure of cloud adoption projects by government organisations in the past three years including any advise shared directly with individual organisations on adherence to the government 'cloud first' policy. Please provide a list showing services and the government organisation that adopted them*

On 27 May 2024, you agreed to refine the third part of your request to:

> *A high-level summary of known obstacles to system level cloud adoption and a system level view of % of agency systems that are cloud enabled.*

Question one: Cloud plans

The Department of Internal Affairs has not received any agency Cloud plans in the past three years. While agencies are required to have such plans for Cloud adoption, they are not required to submit these plans. The Government Chief Digital Officer (GCDO) is responsible for providing the policy, guidance, standards and organising commercial arrangements. Each agency Chief Executive is accountable for the Cloud plans. Therefore, this part of your request is refused under section 18(e) of the Act, as the information does not exist.

Question two: Security, risk or privacy assessments

We have scoped this part of your request to be all 'Cloud Security Risk Assessment Reports'. Please find attached as **Appendix A**, details of ten Reports in scope of your request. I am withholding one of these Reports in full and releasing the remainder with some information withheld under the following sections of the Act:

- 9(2)(a), to protect the privacy of natural persons;
- 9(2)(b)(ii), to protect information where the making available of the information would be likely unreasonably to prejudice the commercial position of the person who supplied or who is the subject of the information; and
- 9(2)(k), to prevent the disclosure or use of official information for improper gain or improper advantage.

Please note that security classifications in the Reports have been redacted to enable the attachments to get through the Department's firewall.

You have also requested all correspondence with these Cloud service providers relating to risks and issues. As it stands, there is a significant amount of documentation within scope and collating this information will impact on the Department's operations. Therefore, we are refusing this part of your request under section 18(f) of the Act, which applies where the information cannot be made available without substantial collation or research.

Question three: Examples of success of Cloud adoption projects

Good examples of successful Cloud adoption projects are provided in Appendix B of the Benefits of Cloud Computing and New Zealand Case Studies, pages 3 to 4 of the Cabinet material: www.dia.govt.nz/diawebsite.nsf/Files/Proactive-releases-2023/$file/Proposals-for-refreshing-the-Cloud-First-Policy-and-strengthening-cloud-adoption-across-the-public-service-16-May-2023.pdf.

Question four - Known obstacles to system level Cloud adoption and % of agency systems that are Cloud enabled

Barriers to Cloud adoption

New Zealand government organisations face several key obstacles to system-level Cloud adoption. The main constraints are related to high levels of technical debt, security concerns, and underinvestment.

For many years, one major issue for public service departments has been "offshoring" and the lack of in-country Public Cloud Data Centres. Additionally, Māori and Iwi concerns related to data sovereignty and jurisdictional risks with foreign-owned Cloud providers add further challenges. Some of these barriers are likely to be addressed as New Zealand experiences significant investment in locally hosted hyperscale Public Cloud Data Centres.

Currently, the major barriers are the low levels of investment in government digital infrastructure and the limited coordination of Cloud investment across the public service. Agencies transitioning from on-premises to Cloud systems report that limited Operational Expenditure (OPEX) presents financial challenges vs. the traditional Capital Expenditure (CAPEX) model that owning your own, on-premise data centre uses. Additionally, the public service capability and capacity to manage multiple Cloud transitions is limited, contributing to slower adoption levels.

Cloud enabled agency systems

Out of the systems in scope for the GCDO mandated agencies, about 38 percent are Cloud-based.

Public Interest Considerations

As is required by section 9(1) of the Act, I have considered whether the grounds for withholding this information are outweighed by other considerations which would make it desirable, in the public interest, to make them available. In this instance, I do not consider that to be the case.

Access to the Ombudsman

You have the right, under section 28 of the Act, to seek an investigation and review of this response by the Office of the Ombudsman. The postal address is PO Box 10152, Wellington. Alternatively, you can phone 0800 802 602 or email info@ombudsman.parliament.govt.nz

Proactive release of your request

The response to your request will be published online at www.dia.govt.nz. This letter, with your personal details removed, will be published in its entirety. Publishing responses increases the availability of information to the public and is consistent with the Act's purpose of enabling effective participation in the making and administration of laws and policies and promoting the accountability of Ministers and officials.

Nāku noa, nā

Jeremy Cauchi
Director Ministerial and Monitoring

Appendix A

#	Document description	Document date	Decision (Release, withhold or partial release)	Applicable withholding grounds under the Act
1	ICT Shared Capabilities Telecommunication as a Service Risk Assessment Report	August 2021	Partially released	9(2)(a), 9(2)(b)(ii), 9(2)(k)
2	Public Cloud Infrastructure as a Service (IaaS) Risk Assessment Report	October 2021	Partially released	9(2)(a), 9(2)(b)(ii), 9(2)(k)
3	ICT Shared Capabilities Marketplace – Managed Payroll Services Security Risk Assessment	29 April 2022	Partially released	9(2)(a), 9(2)(k)
4	ICT Shared Capabilities Marketplace – Payroll Enterprise Software - Security Risk Assessment	29 April 2022	Partially released	9(2)(a), 9(2)(k)
5	GCDO – Microsoft Azure and Azure Active Directory Security Risk Assessment Report	30 August 2022	Partially released	9(2)(a), 9(2)(b)(ii), 9(2)(k)
6	GCDO – Amazon Cloud Security Risk Assessment Report	6 September 2022	Withheld in full	9(2)(b)(ii), 9(2)(k)
7	GCDO – Microsoft 365 Security Risk Assessment Report	12 September 2022	Partially released	9(2)(a), 9(2)(b)(ii), 9(2)(k)
8	GCDO – DaaS Security Risk Assessment Report	30 November 2022	Partially released	9(2)(a), 9(2)(k)
9	ICT Shared Capabilities ITSM Risk Assessment Report	September 2023	Partially released	9(2)(a), 9(2)(k)
10	Infrastructure as a Service (IaaS) Security Risk Assessment Report	November 2023	Partially released	9(2)(a), 9(2)(k)